STANDING COMMITTEE ON PUBLIC ACCOUNTS

Hansard Verbatim Report

No. 46 – April 3, 2007

Legislative Assembly of Saskatchewan

Twenty-fifth Legislature

STANDING COMMITTEE ON PUBLIC ACCOUNTS
2007

Mr. Elwin Hermanson, Chair
Rosetown-Elrose

Ms. Joanne Crofford, Deputy Chair
Regina Rosemont

Mr. Lon Borgerson
Saskatchewan Rivers

Mr. Ken Cheveldayoff
Saskatoon Silver Springs

Mr. Michael Chisholm
Cut Knife-Turtleford

Mr. Andy Iwanchuk
Saskatoon Fairview

Mr. Kim Trew
Regina Coronation Park

Published under the authority of The Honourable P. Myron Kowalsky, Speaker

[The committee met at 10:30.]

Public Hearing: Information Technology Office

The Chair: — Good morning ladies and gentlemen. I call this meeting of the Public Accounts Committee to order and welcome each one of you here. We have only one item on the agenda this morning, and just so you can be prepared, that's chapter 6 of the 2006 report volume 3. The title is Information Technology Office. I also would inform the committee that there is one substitution. Substituting for Lon Borgerson is Mr. Ron Harper, so we welcome you, Mr. Harper, to our committee.

And we will follow our normal procedure. We will ask the Provincial Auditor to quickly review chapter 6 with us this morning. From the office presenting we have Jeff Kress, principal. Following that brief overview, I would then ask the deputy minister and chief information and services officer, Mr. Don Wincherauk, to introduce his colleagues and respond, again as briefly as possible, covering the material involved. And then we will have time for questions from the members of the committee. So with no further ado, we will give the floor to Mr. Kress.

Mr. Kress: — Thank you, Mr. Chair. Good morning everyone. As noted, I am here today to discuss chapter 6 of 2006 volume 3 report. The chapter describes our audit work and findings on the Information Technology Office or, as I'll refer to it in the presentation, the ITO.

In this presentation I will include two parts. The first part will describe the ITO's processes, the secure data centre. The second part of the presentation will identify the progress the ITO has made to manage its IT [information technology] service delivery. The ITO provides information technology to client departments. At the time of our report, 15 government agencies had services provided by the ITO. When a client joins the ITO, the ITO becomes responsible for hosting and managing client systems. Also client IT staff become ITO staff.

The purpose of our audit was to ensure the ITO had adequate controls to protect the confidentiality, integrity, and availability of client information technology systems and data for the period October 1, 2005, to March 31, 2006. We used four criteria for this audit.

The first criteria was that the Information Technology Office needed to show management commitment to security. For example, roles and responsibilities need to be clearly defined. Risks need to be identified, assessed, and managed. Also management needs to have process to actively manage security.

Secondly the ITO needed to protect clients' systems and data from unauthorized access. This would include the need to have adequate physical controls for key computer equipment. Also the ITO needs to have logical access controls to protect systems from unauthorized access.

The third criteria was that the ITO needed to have clients' systems and data available for operation when needed. To have good availability, the ITO needs to do regular backups of data. The ITO also needs to be prepared for significant failures by having a complete disaster recovery plan available for use.

Our last criteria was that the ITO needed to protect the integrity of client systems and data. That means having good processes to manage IT systems and to ensure that changes work as planned.

We found that the ITO had adequate controls except for four recommendations. We recommend that the Information Technology Office perform quality assurance tests to ensure its security policies and procedures are followed. We recommend that the Information Technology Office follow its security policies and procedures. We recommend that the Information Technology Office protect its systems and data from security threats. And our last recommendation, we recommend the Information Technology Office have a disaster recovery plan for its data centre and client systems.

The second part of our audit was a follow-up on a prior report related to service delivery. We found that the ITO needs to continue to improve its service delivery processes. We therefore continue to recommend the ITO sign service level agreements with clients prior to delivering information technology services. We also continue to recommend that the ITO sign agreements with clients, that address security and disaster recovery processes, expectations, and reporting requirements.

In conclusion I'd like to thank the ITO for their co-operation during these audits.

The Chair: — Thank you very much, Mr. Kress. And just for clarification, I have one question before we move to Mr. Wincherauk. You said the client IT staff become ITO staff. Does that mean then that they are paid employees of the ITO department and that they are fully answerable to ITO, or are they seconded from the department and still paid by the department that they originally worked for? I'm not clear on that, and it wasn't clear from the chapter.

Mr. Kress: — No, it's a very good question, Mr. Chair. The staff do move to the ITO and become employees of the ITO. In the year in which the transition occurs when there is . . . the new contract is done, there might be something midway through the year to figure out what costs should be for the department and the ITO, and that just ties in to where the estimates and who received the funding.

The Chair: — Thank you for that clarification. I'm sorry to interrupt. We will give the floor to Mr. Wincherauk and again if you'd like to introduce your colleagues and respond, we would appreciate that.

Mr. Wincherauk: — Thank you very much. I have several ITO staff with me today: Rory Norton, assistant deputy minister of corporate information services; Richard Murray, our executive director of policy and planning; Fred Antunes, executive director of corporate and customer service; and Carla Feld, directly behind me, who is our director of business development.

As we are the youngest department in government and development of our youth is one of our top priorities, Troy

Smith, one of our new financial analysts, has joined us this morning to obtain some experience with the public accounts process. This is Troy right here.

Since July 2004, the ITO has been consolidating IT service delivery across executive government. One of the benefits of a consolidated IT environment is better security. We take the auditor's reviews and recommendations very seriously. We believe that strong processes for managing IT security are critical to protect government systems and information because of the number of threats are increasing at an alarming rate.

As an organization we've been undergoing a tremendous amount of change, but we still manage to do a lot of work on improving IT security. The Provincial Auditor's detailed review has provided an independent evaluation and validation of the work we've done to implement the building blocks required to create a secure IT environment. While we've made a lot of progress over the last two years, we also recognize that there is much more work to do.

I am pleased that the Provincial Auditor found that we had adequate controls to protect the confidentiality, integrity, and availability of our clients' IT systems. The Provincial Auditor confirmed that we have some well-established security process. As an example, we have an effective IT organization that clearly outlines responsibility for security, develops strong security policies and procedures based on international standards, implements strong physical security controls to protect our IT infrastructure, develops strong controls to prevent unauthorized access to client systems and data, and perform vulnerability testing on the data centre to identify security weaknesses.

We agree with the four recommendations made by the Provincial Auditor, and over the last year we have made progress on addressing the issues identified in this audit. The auditor is just finishing a second detailed IT security audit, and we anticipate that the next report will recognize these improvements.

I'd also like to touch on some of the ITO's other accomplishments over the past year. The IT service partnership initiatives has been progressing well with the ITO now providing IT services to 20 government departments and agencies. The departments of Justice, the Department of Corrections and Public Safety, and the Department of Community Resources have just recently joined our partnership. I am proud to say that we are now providing IT services and support to over 90 per cent of executive government staff.

When complete, the benefits of this initiative will include better service to the public and cost savings to the taxpayers. We'll eliminate 11 help desks. There will be 35 fewer server locations and 15 fewer server rooms which will also help increase security. A properly equipped server room costs between a quarter and three-quarters of a million dollars. We'll eliminate over 250 aging servers. A typical server costs between 8,000 and $10,000. The average cost per user will be reduced by 7.5 per cent.

Last fall our IT service delivery partnership initiative was awarded the Gold Medal Distinction Award at the government and technology conference in Ottawa. That award is a testament not only to the importance of the project itself, but the skills and knowledge of our employees.

We've also developed a new governance and approval process for IT expenditures that's already benefiting government through introduction of better decision making around corporate expenditures for technology. There are clear benefits from IT consolidation. The security of government information assets continues to be a priority of the office as we are now detecting and dealing with some 20,000 security threats a day on our firewalls.

We've developed an information protection guide to classify information based on sensitivity. We have signed security memorandum of understanding with 10 of our partner departments, and we expect to have all the remaining partners sign within the next several months. This MOU [memorandum of understanding] provides assurances that government departments understand and are adhering to the security standard.

I'm proud of the accomplishments of my staff over the past two years in improving government IT processes, reducing costs, and in improved protection of information assets in our care. And I look forward to your questions now.

The Chair: — All right. Thank you very much for that summary, Mr. Wincherauk. We'll open the floor to questions. I see Mr. Dan D'Autremont, the Sask Party critic for the Information Technology Office. Mr. D'Autremont.

Mr. D'Autremont: — Thank you. I'd like to welcome the deputy minister and his officials here today. We have discussed ITO many times in the past and we'll continue to do so, I gather.

The Provincial Auditor has reported that he found adequate controls except in four specific locations, so I direct the question to the Provincial Auditor's office. In your first recommendation that the ITO perform quality assurance tests, what kind of tests were you looking for them to be performing?

Mr. Kress: — That's a very good question. The purpose of the recommendation is to make sure that the ITO can know that its policies and procedures are being followed. For example, one of the processes that the ITO has as a policy to make sure that it checks for stale accounts, i.e., those are accounts for people that haven't used them for a certain period of time. The reason why that's a very good control is because it helps to identify whether users who may have left an organization are having their access removed on a timely basis. This ensures that only authorized users would have access to those systems. So as an example of a quality assurance test would be to have something like perhaps an internal audit unit that would go through and do a test to make sure that the ITO had actually followed that policy and procedure.

And there are lots of other similar types of tests for change management, for user access, just to make sure that those policies and procedures that are established and have been identified to be followed are working effectively.

Mr. D'Autremont: — Okay. Thank you very much, Mr. Wincherauk. Has ITO, since this report came out, instituted that kind of a process where you are going through all of the various departments to ensure that people who are no longer there or whose status has changed have the appropriate level of access?

Mr. Wincherauk: — I'll ask Mr. Norton to speak to that.

Mr. Norton: — Yes. We have processes now in place. I think one point about user access and when they leave the departments, we have a process that's service request which is about adding new users and removing users from access, that departments should be signing off when an employee leaves to say yes, this person's leaving and we remove access.

On occasion this doesn't happen, and that's where the stale account process which Mr. Kress was talking about is now in place. We have a process that we look for accounts that have not been accessed for 60 days, and then we will take that list and provide it back to the department to say, is this individual still with you? Could be on vacation, a longer vacation, or maybe a sick leave or that thing, so that's validated through that. But we run that process every two weeks now.

Mr. D'Autremont: — When an employee of a department exits that department, is part of their exit paperwork that the department would go through an indication to ITO to remove them from the active account list, or is it somewhat more haphazard than a formal part of the exit process?

Mr. Norton: — Different departments may treat it differently as a formal part or not. But I think it is pretty much formal in most departments to have what we call a service request form filled out that will say this employee is leaving. That allows us to remove all their rights from systems, go collect their computer and wipe it clean and redeploy that device. So yes, that is done.

Mr. D'Autremont: — When you say that most departments but not all may be doing this on a formal basis, are you approaching those departments to ensure that that becomes a part of their procedures?

Mr. Norton: — Absolutely. From the IT part of the exit procedure, it is a requirement. So it is required of departments to do it, and they understand that, and we have communicated that with them.

Mr. D'Autremont: — Since you have communicated it to them, are they doing it?

Mr. Norton: — Again when you say formal, I mean is it integrated in their HR [human resources] formal process? I have not checked to that end. But again when people leave the departments, all departments are aware that this form is to be filled out to delete their account and to clean up their file rights.

Mr. D'Autremont: — Well they may be aware of it within the IT section. It may not necessarily . . . that everybody is aware, the supervisors, when somebody exits. But if it was part of their formal exit package that this was one of the items that had to be completed and checked off and then forwarded to ITO, it would then become a standard part of the process rather than a more haphazard if somebody remembers to do it, it happens.

Mr. Norton: — Again my indication is that most departments do have it as their formal part of their exit policy. I have not validated that completely, but again it is on a regular basis that all of them use it and understand the process.

Mr. D'Autremont: — It's maybe something that the Provincial Auditor's office in their reviews could look at perhaps, that the other departments are following through on this and that is a formal part of exit strategies from a department.

The Chair: — Perhaps if the Chair could interject, whose responsibility is it to validate that? Is it the department, the other departments, or is it your responsibility to ensure that that's validated, or do you know?

Mr. Norton: — Again I think that the onus is always on the department in our service level agreement to tell us when people come or go. We have no indication of that happening. We do use the stale account process to make sure that there isn't some that have been missed inadvertently that we do clean up later.

The Chair: — Mr. D'Autremont.

Mr. D'Autremont: — Thank you very much. The tests that you carry out — stale accounts as an example — what about tests for physical security? What about tests for logic security? I'll direct this again to the Provincial Auditor's office. What are you looking for in that particular area of physical security or logic security within ITO and the departments they work with?

Mr. Kress: — Once again, for physical security it would be the same types of controls that we look at as part of our audit, for example, making sure that facilities are properly locked, that only authorized users would have the keys or cards or whatever access required. For example the ITO has a large data centre out by the University of Regina, but they also have a number of other data centres that it has throughout the province. Those are used for backup sites or for storage of other information. So it's important to make sure that those facilities are properly secured. Now we did our audit. We found the physical security, especially around the university site, was very strong. And so that was one element that was quite good

There are other areas. You asked about logical access controls. For example the ITO has standards for minimum password length, composition, how long passwords need to be changed by to make sure that security is going to be good. So when we did our audit, we found some cases where security standards were not being followed. So the ITO would have had policies and procedures to say, make sure all passwords were changed within a certain period of time or to make sure that change management — that's when a system is changed or updated — to make sure that those changes are appropriately tested and approved prior to them being implemented. So from a quality assurance perspective, there are independent tests that can be done to review to see whether or not those policies and procedures are working effectively.

Mr. D'Autremont: — Thank you very much. Mr. Kress talked about password security and length of the passwords. When

you're making a standard change of passwords across the whole system or a requirement that they be changed within a certain period of time, when a person goes through your system and changes their password, can they change it to the same password they already are using?

Mr. Norton: — No they can't.

Mr. D'Autremont: — Does it have to be a significant change from the previous password to the new password? So if their password is dog and they put two g's in it, is that a significant enough change to allow that password then to be accepted?

Mr. Norton: — I wouldn't say it goes out for significant change. It looks for change, but it requires a strong password, meaning that we use, you know, multiple characters, numerals, capitals, things like that to make it. So again I could change from, you know, say dog to — well dog wouldn't be valid — but dog with a couple of numbers and other characters to dog with another d in the front and that would be viewed as a change.

Mr. D'Autremont: — If they . . . and I don't know what your time frame for change is but let's say it's every two months. So this month I have password A. I change it to password B. In the third series can I change it back to password A?

Mr. Norton: — No. The password change time is every 30 days and no, you can't change it back. It won't allow you to repeat, I think it's 15 or 20 of your last passwords.

Mr. D'Autremont: — So somebody just can't keep flipping back and forth and then if somebody gains access to that password through some means then at some point in time they still won't be able to access.

Mr. Wincherauk: — Just one thing we've noted as we've been now doing this for two and a half years, there's really a tremendous education part of this where you actually have to go back out and educate people that this is why you have a password. This is why your screen will click off after, I can't remember how many minutes it is, and then you'll have to re-enter. We find a lot of the people we provide a service to don't like it, and one of the reasons is that they simply don't understand how important it is. So we've taken it upon ourselves to make sure that we now go out and when we're dealing with the partnerships educating about why this is so important.

Mr. D'Autremont: — On the physical security side, I'm assuming from the auditor's report and from your assurances that physical security of somebody entering is reasonably secure. Would that be the case?

Mr. Wincherauk: — Maybe Mr. Norton can speak to what we actually do at our facility at the University of Regina.

Mr. Norton: — Yes, absolutely. I mean around our data centre and any of our key systems, I mean they're all under secure card access. Only our main data centre . . . You feel a little bit like *Get Smart* going in there. You go through about four different doors and a few pass keys to even get close to the data centre. So there's a lot of security around those pieces.

Mr. D'Autremont: — Do you have security in place for internal security in the sense . . . There was a piece in the paper that happened here in Saskatchewan. Now I don't know what it'd be — eight, ten years ago maybe give or take a couple of years — that somebody walked out of a secure data centre with a hard drive, not for nefarious means to exploit the information on there but for other reasons. Do you have security in place to assure that that doesn't happen?

Mr. Norton: — Absolutely. And again part of that is we have video surveillance that is monitored anytime anybody comes into an area, even relating to change as Mr. Kress had referred. If someone goes into the server room and touches a server, we're looking to see, do they have authorization to make that change or to be even in there. So again we are monitoring it in a number of ways like that.

Mr. D'Autremont: — Do you monitor people within your system internally accessing information and making attempts to copy or replicate that information or transmit it outside?

Mr. Norton: — Yes, absolutely. I mean transactions within our environment are audited, and we can follow the path of things like that, absolutely.

Mr. D'Autremont: — Okay, thank you very much. When you give someone access to your system through either ITO itself or through the departments, what kind of security do you have in place to ensure that the person gaining the access has the appropriate level of access and doesn't in some manner exceed that and access information that they have no authority to access?

Mr. Norton: — Access control is directed from the departments. We really don't give any access to anything without a department form, again, which we call the service request would come over to say this is the type of access the person requires and who they are. We then audit you know what is in a particular file rights and give that back to what we call service approvers. So these are the people who are providing the access on a regular basis to ensure that people have the appropriate access and there's been no errors in access given to people.

Mr. D'Autremont: — Have you had any difficulties where someone with an entry level access has been able to access something that they should not have been able to because they did something?

Mr. Norton: — I'm not aware of any incident like that, no.

Mr. D'Autremont: — Okay. The auditor's second recommendation is that the ITO office follow its security policies and procedures. In what cases did ITO not follow — I'll ask this to the Provincial Auditor's office — in what cases did ITO not follow its own security policies and procedures?

Mr. Kress: — One good example would be change management. The thing with technology is that systems are changing all the time, and there are new risks and new threats that occur on a regular basis. To make sure that those threats and risks are going to be appropriately addressed, companies will often come up with updates to systems.

Also when new changes need to be made to a system for new functionality, there'll be changes done to a system. To make sure that those changes are going to work as planned and that the integrity of the system and the integrity of the availability is going to be there, there needs to be very good processes to, first of all, document the changes to make sure the changes are appropriately approved, to make sure the changes are properly tested. As an example, if an unapproved or untested change went through, that could impact the way a system worked or it could impact the availability of the system.

So when we tested that process, we found the changes weren't documented. We found a lack of approval for some changes, and overall, that the process wasn't being effectively followed.

Mr. D'Autremont: — Thank you, Mr. Kress. Mr. Wincherauk, how do you respond to those that the changes were being made that were undocumented and without approval?

Mr. Norton: — Again I think some of this . . . Again we have very rigorous change processes that have been put in place. And again our growth with the number of staff over the last few years has also been an education for our people.

When we looked at the changes that the auditor had highlighted to us, many of them were what we call our low-risk changes which are, you know . . . The backout is pretty understood, our staff being of the routine nature of knowing that is a simple . . . a change to them that wouldn't require a ton of documentation on the backout because it's pretty routine what the backout would be.

That's where we had a number of issues. We've created templates for those type of changes so that, you know, that information is for sure captured and validated.

Mr. Wincherauk: — And also, I think that as you move from being an organization where we were, you know, 60, 70 FTE [full-time equivalent] to an organization as large as we are right now, you have to start imposing these processes on your organization, where in the past everybody seemed to know each other so well; we'll just fix it now and move on. Well we have to have a lot more rigour and discipline in our system than we had in the past.

Mr. D'Autremont: — Well absolutely. And when you start customizing a system without documentation, as soon as the person that fixed it leaves, you no longer have the ability to operate the system.

One of the things that happens with software and programs when you're customizing them, quite often the administrator will, there'll be back doors built into the system. What has ITO done to assure that there either are no back doors or that the back door accesses are very, very strictly controlled?

Mr. Norton: — With all new custom development, security is a big part of that in the risk analysis of the information, as well as our staff have people who are doing the coding. We also have people who are reviewing the coding and looking through it for issues with coding, looking for things such as vulnerabilities or back doors or whatever you call them have been put in. So again, that's a regular part of any application development you do. One, just focusing on the security and risk and identifying what is the data, what is the system? You know, how much more rigour has to be put into finding these things. And then, code reviews will find most if not all of those.

Mr. D'Autremont: — Does ITO have a policy in place to exclude any back doors in any of their software?

Mr. Norton: — Well absolutely. I mean, back doors wouldn't be a common . . . We wouldn't provide back doors. I don't think there's any value for a back door. We'd make a front door that's secure and accessible.

Mr. D'Autremont: — Microsoft seems to think that back doors are good, which causes a huge problem for everybody running Microsoft. But other programs' developers allow themselves easy access, that they do not have to go through all the steps to be able to go access a system to make changes that are needed and it makes life easier for the programmer, but it makes the system less secure.

Mr. Norton: — And again, access to systems where developers are building them and have ready access to them is one thing. Once they go into production environment, the developers don't have an access. If there's any type of intrusion from unauthorized persons such as a developer who has tried to create something like that, we would be aware of that.

Mr. D'Autremont: — Okay. Thank you. The auditor's third recommendation is that the ITO office protect its systems and data from security threats, and that's obviously what we're talking about now. But to the Provincial Auditor, what threats did you detect that ITO needs to further protect itself from?

Mr. Kress: — The threats that we're talking about are the threats that exist out there to any organization whether it be in government, external, or even to home computers. There are viruses out there. There are people that attempt to break into computers to either try to change systems, obtain confidential information. So there are lots of threats out there, just sort of in the environment with the Internet and the accessibility of information, the rate at which these things can move throughout the world.

So our recommendation is really focused on the ITO's processes to monitor its systems, to be able to identify if someone is trying to get into their systems or if some threat is possibly going to be able to breach the security.

Mr. D'Autremont: — Did you detect any instances or threats that were more serious and more likely to penetrate or did penetrate ITO's security?

Mr. Kress: — We didn't, but it's a difficult question to answer and the reason being is the sheer volume of hits that are occurring on some of these systems. We're talking about many, many thousands of transactions in some cases, if not potentially millions of transactions a day. So you wonder maybe how could somebody possibly monitor that with what's happening. Well there are tools and other software available to help to identify and sort of filter out what maybe I'll call noise, to separate what is actually a potential security threat and what isn't a security threat, what is just part of normal operations that we're going to

see and we can accept.

And I think part of our recommendation, the reason for it, was that the ITO didn't have those tools working effectively to be able to identify what was noise and what was a security threat.

Mr. D'Autremont: — Again to Mr. Kress. Google will often ping a site on a regular basis. Do you consider that to be noise, or is that a security threat?

Mr. Kress: — As a general rule, anything that would be non-invasive trying to break in would probably be considered to be noise. There are lots of different sites that will provide lots of hits and that's why the systems the ITO has might have anywhere from thousands to millions a day. The type that we're talking would be threats, might be more detailed attacks, hackers, or maybe specific virus threats that are trying to get through their systems. So no, I wouldn't consider Google to be a security threat with a simple ping.

Mr. D'Autremont: — Thank you. Because there's lots of organizations that do those kind of pings as well, and for various reasons.

I'd like to move on to the disaster recovery system. Disaster recoveries for an operation like ITO and the departments are critical for the continued existence of those files. We've moved away from reliance on paper as a backup system to electronic data, and if that system is lost then everybody's data is lost and access to various things. We know all we got to do is take a look at whenever the ATM [automated teller machine] doesn't work or the card reader at the local store where you're making a purchase. It disrupts everybody's life when that doesn't happen. So it's much more critical when all of your personal information that is stored by government for health care and various other things has a potential for failure.

What has ITO done to assure that the proper redundancy is in the system, that the data is stored in more than one location, that there is security at all of those locations for not only just the physical threat of somebody accessing it and acquiring information or . . . [inaudible] . . . but have you even looked at things like protection from EM [electromagnetic] pulses and those kind of massive potential disasters?

Mr. Norton: — Well first of all, I mean, we do have multiple sites that we can go to in the event of a disaster. We have a site that replicates data real time right in Regina to a location that would allow us to make a faster restore if we had to of the core services, not of all systems. And we also have an off-site location in Swift Current where we would go if there was an issue, with a larger issue, with all of Regina or something like that.

We are also working hard on developing a disaster recovery site somewhere — possibly in P.A. [Prince Albert] or somewhere along there — to provide, you know, a far distance as well as replication to that site. So rather than have the replicated site in Regina it would be up in Prince Albert.

We do backups as a regular basis, backups, and test those backups to see that they can be restored, of all of our systems. Tapes go off-site daily, but we also keep copies of those tapes locally so that we could restore in a quick manner as well.

Our core systems, our disaster recovery target is seven days in the event of a major disaster for our core services. And services that haven't been defined as departments through their business continuity plans will have specific times to be up as well, related to them.

You know another thing that we do is threat and risk assessments. I mean we did six in the last 18 months, threat and risk assessments of our locations to ensure that, you know, again from a physical ways, from an electronic manner, that those systems are secure.

Mr. D'Autremont: — Seven days to return core services seems to be a bit long. How does that compare with other jurisdictions and other industries?

Mr. Norton: — Again that is in event of a major issue like, again, if our data centre was taken out completely, where we had to source equipment to get those core services and replace that all and build that up. I think again that's why we are looking for certain systems to have the redundant site in a P.A. or something. But again if only the data centre is hit, we're still up because we have a location in Regina. It would be a major disaster that would take us to that end.

Mr. D'Autremont: — Well we have seen major disasters. And I don't mean in the sense of 9/11, but with the brownout in the eastern US [United States] which covered a huge geographic area. What kind of an impact would that have on ITO and the services it provides to all the government departments?

Mr. Norton: — Well obviously that's going to be affected as well as, you know, the client systems wouldn't be accessing any of the people. But I think it comes back to business continuity plans of departments. And as we went through in Y2K and that, do we have ways to deal with transaction and doing business outside of the electronic systems being available? Again we can see how seven days seems like a long time, but again, given what we're trying to rebuild, it isn't that long of a time, yes.

Mr. Wincherauk: — I think as we move forward in this fiscal year, we have plans to bring forward an initiative that would see a second data centre that would have to be 250 kilometres away from Regina so that we do have complete redundancy.

Mr. D'Autremont: — Okay. When you're doing the testing to ensure that your security is safe, do you utilize the services of independent third parties that are not tied in with ITO and not tied in with any of the departments that they can utilize their expertise to try and access ITO or any department's information?

Mr. Norton: — Yes, we do those with third parties. We don't do them ourselves. We employ people to come and do them for us, yes — or contract.

Mr. D'Autremont: — What has their success or failure rate . . . Success for them would be to access and failure would be failure for you. So have they managed to access any of the systems other than the initial entry?

Mr. Norton: — Again, no specific access. They did identify some threats that we should be aware of that are potential issues, but there was no particular access that they were able to crack in or get in without proper credentials.

Mr. D'Autremont: — Have they, the third parties that you may employ in this . . . I was talking to one third party person involved in this industry — and that wasn't involving ITO or government — but was simply able to walk into an office and gain access to their system just by talking to people. Are your people made aware of those kind of potential security risks?

Mr. Norton: — Definitely. The IT people in all of our areas that IT people exist are secured areas, and they are instructed to challenge anyone that they don't recognize or that doesn't have proper picture tag or stuff like that. Yes.

Mr. D'Autremont: — One of the things that you see major IT services face from time to time is denial-of-service attacks. Has ITO faced that or are you prepared to face that kind of an incident if it should occur?

Mr. Norton: — Not to my knowledge have we ever had a denial-of-service attack against us. But absolutely we have methods to be able to counteract that.

Mr. D'Autremont: — How do those methods compare to other large industry sites that actually have been brought to their knees through that? And these are major corporations.

Mr. Norton: — I cannot speak to specific individuals, how they deal with it. Again I think the processes we would use would be similar to that used by other large firms — maybe not the ones you specifically talk about, but ones that are more successful.

Mr. D'Autremont: — Thank you. Well some of these were very major corporations and faced the loss of their service and their customers couldn't access their services. I mean, I have no idea why people do this, but they do it. And so you need to be able to . . . How would you differentiate though between someone involved in that — or a computer involved in that — and somebody who is legitimately trying to access the system?

Mr. Norton: — As Mr. Kress had noted, we do have intrusion detection systems that actually tell us people are hitting at us. Again, we get between 20 and 35,000 potential security threats a day that are analyzed through this intrusion detection system. So it identifies, you know, is this valid traffic, someone trying to do legitimate business with us? Or is this someone who's just trying to feel us out, trying to do harm to us?

Mr. D'Autremont: — Okay. Thank you. The second part of the auditor's report deals with service agreements and the service agreements between ITO and its clients. And although it's, Provincial Auditor is recommending, it's not an official recommendation it looks like to me in the report, under page 218. So I can address this to the Provincial Auditor on page 218 under "Signed service level agreements required" and it says:

> We . . . [recommend] the ITO sign service level agreements with its clients prior to delivering information technology services.

The other recommendations are numbered, but these in this section are not. Are they official recommendations or are they sort of a wish list?

Mr. Wendel: — Yes, Mr. Chair. These recommendations were considered by the committee last year.

Mr. D'Autremont: — Okay.

Mr. Wendel: — And the committee agreed to them. But this was a follow-up to see how far the department has come along in implementing those recommendations, just information for you to know how far they've gotten.

Mr. D'Autremont: — Okay. Thank you very much. So has the department then put in place all of the necessary service agreements so that both ITO and the clients know what is expected of them, how to measure the success or failure levels, and who is responsible for what particular items?

Mr. Wincherauk: — I'll ask Mr. Antunes to speak to this.

Mr. Antunes: — Yes. So right now we have 16 departments that we provide a full range of services to. Nine of those 16 departments have signed service level agreements. There's a couple this past year that their signed agreement expired, and we're in the process of renegotiating those. There's, I think, two departments that have been in for about six months that we're continuing to actively negotiate with those departments. And there's three other departments that recently joined us in the last six months that we're negotiating with on again a weekly basis, I guess, to try to get them to the point where they have a signed service level agreement.

And I guess, just as we were going through with the Department of Community Resources — so in, I guess, picking up on the recommendation — the Department of Community Resources actually signed a service level agreement before they decided to join the ITO. So we have made some progress in this area. We've also tried to simplify the service level agreements to make it easier for them to articulate what their business requirements are. So we've made a number of steps to try to work with the departments on that.

Mr. D'Autremont: — Well I think it would be important, would it not, for ITO to understand what the department needs for services. And you would do that through negotiation and a service agreement before you actually enter into the operation because how do you make the transition from what the department is doing to what ITO will be doing if you don't clearly understand what each other's needs are?

Mr. Antunes: — Yes absolutely. And I think we have a standard service level agreement that, you know, we present to the departments at the time that we're undertaking the discussions. So they have a general, I guess, understanding of what it is exactly that they're going to get from our base services. And most departments are saying yes okay, from a base service perspective, that's acceptable to us.

I think what gets more difficult for them is actually having to go back and say okay, well for a specific application, well how fast do I want this thing restored or who do I want to be able to have

access to it, and those types of things. So in most cases the departments have to go back to talk to their program staff and get to the point where they can say — and clearly put down on paper for the first time — this is specifically, you know, what services I need and when I need them and that type of thing. So it's more on the application side than the routine services that we deal with, where the departments have to go back and do some homework, I guess, to kind of flush out those requirements.

Mr. D'Autremont: — So is this more a security need — like what kind of security, who has access, talking about the stale accounts, and those kind of things. Or is it the actual operation and data collection within the department?

Mr. Antunes: — I think it can be both. I mean some of the security requirements are, you know, who should have access and how fast should the thing be recovered and those types of things. So we're asking the departments to clearly identify, you know, what are their disaster recovery requirements. How fast do they need to . . . would we need to restore them or that type of thing if there is an event of a disaster? Other things could be, you know, we work from nine to five in terms of when our — sorry, eight to five — from our help desk so they may want extended hours on weekends. So it's defining at what times of the year do they want those extended hours? Who do they phone and those types of things and what the service . . . how much that would cost them for extended services. So it can be a range of things that we would work with them on.

Mr. D'Autremont: — When you're taking over a new account with another department, would they not already have significant number of those things in place?

Mr. Antunes: — They do but sometimes they're not as formal as maybe in the past. So what they may have had is an IT organization, and they know somebody's phone number, so they're able to phone that person, and then that person can come in and do something at the office, that type of thing. So when we're dealing with, you know, 7,000 clients, we want something a little more structured.

So they know that we have one phone number, 7-5000, for the help desk so that they can phone us during work days. But then it's putting in place the process that says, okay on evenings and weekends this is the number that you can call and here's how fast you want us to respond. Do you want somebody to be available so that they can come into the office or to be on-site to actually fix something within 10 minutes, or can we have half an hour or an hour or that type of thing. So it's actually formalizing and putting down on paper exactly what they expect from us.

Mr. D'Autremont: — Okay thank you. When you enter into either a formal agreement, or let's say before the formal service agreement takes place, how is responsibility assigned for security, for any security breaches? Is it the department's responsibility? Is it ITO's responsibility if that service agreement isn't in place?

Mr. Norton: — So I would say we generally have the service agreement that is a template and that is what we operate by even without a signed agreement. There's a number . . . There's an appendix called appendix A that covers off most of the security things you're talking about and all those important items. That is the base agreement that we operate by even prior to signing any of the substantial detail and department-specific things.

Mr. D'Autremont: — So if there's a security breach in a department that does not yet have a service agreement signed but simply has looked at the template, who then becomes responsible for that? Is it ITO? Is it the department? Who answers the questions on the security breach? Which minister takes responsibility or should be taking responsibility for it?

Mr. Antunes: — Yes I think it depends on where the security breach came from. So if it's a security breach where somebody's accessed our systems, and we have processes in place that we have articulated to the department of how we're going to protect the integrity of their data and some of the things that the Provincial Auditor's talked about this morning, I mean that's clearly our responsibility to do those types of things.

But if it's a department that has a policy in place where they don't lock down their offices and somebody can walk in off of . . . you know, kind of into their office and they've got their password stuck on their monitor and they can sit down at the computer and start typing and they do something, I mean then that's a department responsibility. So we can put in place all the processes around, you know, having strong passwords and things like that, but if the users don't understand how to use those processes or why they're as important as we talked about earlier, then they can be the people that allow that security threat to happen.

So I think it would depend. And those roles and responsibilities, I mean, are defined as we go through the process, and we have discussions with the departments.

Mr. D'Autremont: — So when it depends, does that mean it would take a court to make a decision if somebody's personal information is allowed out into the public for some reason, some means that . . . and there is harm caused? How is the decision made on who is responsible at the end of the day? Does it rely on the court system?

Mr. Norton: — I think ultimately a department is responsible for the security of their own data. We are custodians and manage and protect that data. So ultimately the department is responsible. Again the agreement with us and process with us is made between a department to ensure that that occurs. But I would say ultimately a department would be responsible.

Mr. D'Autremont: — Do the departments know that?

Mr. Norton: — Absolutely. And that is why they have the people who approve who gets file rights, who is allowed access, at what times of day are access, who's secured from it. So that's all determined by the department. We are custodians filling out that thing. Again we may be at fault at some case in that, but ultimately it is the department who owns the data and is responsible for the data.

Mr. D'Autremont: — Does that responsibility change in any form once a service agreement is signed and completed?

Mr. Norton: — No.

Mr. D'Autremont: — So whether you have a service agreement in place or you don't have a service agreement in place, the lines of authority and responsibility are then clearly known by all parties involved.

Mr. Norton: — Absolutely. Processes and responsibilities and rules have been put in place with any department that we are now doing business with.

Mr. D'Autremont: — Okay. Thank you. I think that's all the questions I have, Mr. Chairman.

The Chair: — All right. Thank you, Mr. D'Autremont. Just for the information of committee members, Mr. Cheveldayoff has left. And, Mr. D'Autremont, you are now substituted in as a voting member of the committee in case you didn't realize that.

Just a couple of questions, and I believe Ms. Crofford also has some questions. But I'm not as knowledgeable about the technology as my colleague, Mr. D'Autremont, and perhaps others around the table. But my reading of the chapter . . . And I was trying to find the exact wording. And perhaps I imagined it; I haven't found exactly what I was looking for. But there was a statement made that there were 20,000 threats a day to your system. And I thought from the auditor, the auditor says that "Without monitoring network alerts, the ITO may not be able to detect security threats quickly." How do you know that there's 20,000 threats, and how soon do you know that?

Mr. Norton: — So I think this is where the auditor and I had many discussions on this point. Again this is about intrusion detection which is basically like a burglar alarm. When someone's in your house, you know it. There's somebody in there.

So we have intrusion detection on the front of our systems, but again most of our focus has been around the prevention of threats, having people attack us inside, outside, doing security threats. We have intrusion detection on our front-end systems, and that's where we are getting these. We are readily seeing these potential attacks.

I think the auditor was concerned about how alerts were coming off and that we weren't just reading everything as garbage because, you know, a ton of information is no information, where it was more screened and alerts were specifically being sent to people. Again we weren't as mature as we are today in that where we absolutely are doing it to a greater extent. There's constant monitoring of that. We're alerted 24-7 if there's any issues resulting in intrusion detection in the area.

The Chair: — So I guess then I would ask the auditor: do you feel that the detection capability of the department is as strong as it needs to be, or do you still recommend that there be stronger detection awareness and defences in place?

Mr. Kress: — We are still in the midst of performing our current audit, so I'll have to leave the point more to . . . At the time of our audit we certainly did feel that the detection systems needed to be stronger. And in a future report that will come to this committee, we'll be updating as to how much those processes have improved and if they are now indeed adequate.

The Chair: — So then I guess I would ask the deputy minister or whoever would answer, what steps have you taken since this audit? Have you added staff? Have you spent more money? And have you added new software or equipment to strengthen that detection system?

Mr. Wincherauk: — Just a couple of general comments, and then I'll turn it over to Mr. Norton. In this area we have to be ever vigilant. The changes that are going on outside there and how hackers work and all that — just staying ahead of them is a major task. And I think we've made some tremendous progress in this, but again I think you can never feel comfortable. You've always got to keep working on this and improving what you have and testing it. And I think that's the realm we're in right now, and we'll continue to be aggressive on that. And I think Rory can speak to some of the details.

Mr. Norton: — Yes, again we didn't specifically add staff to that. I think it was just a focus again on . . . At first we were building more about keeping people out and ensuring that there was no potential . . . And now we've just directed staff that are doing more of the intrusion detection and have expanded that.

The Chair: — Okay. Well thank you, and we'll await the auditor's next report to see they would view this situation. The other question that I wanted to ask in that regard, in regards to security, is you mentioned that you do an audit for unauthorized copying or transmitting of information. Can you just go into a little more detail about what kind of an audit it is? Is this a random audit? Is it a percentage of some factor that you use? Or do you only do the audit when you see some suspicious activity? Or is it some combination of two or three of these?

Mr. Norton: — I would say it is not specifically an audit because again to go through particularly all those logs would be impossible, of access. But definitely when we are made aware of potential situations or potential, we can go back in and look at when things were accessed and by whom.

The Chair: — When did you commence doing this type of audit?

Mr. Norton: — Again certain systems have, you know, for years had that type of functionality in them. Other systems, there are potentially systems that wouldn't have that still to this day, but again the critical systems . . . [inaudible] . . . that have private data, things like that in them, are monitored in that manner.

The Chair: — So since you've been doing this type of audit, let's say, would say the last three years, would that be a fair question to ask? Have you found any breaches of . . . [inaudible interjection] . . . I'm talking about internal breaches, access to information, transmission of information, copying of information. And if so, how many cases, say in the last three years?

Mr. Norton: — I would say probably about three with improper access. It wasn't necessarily that the individual didn't have access to the system but in fact accessed it at inappropriate times or an inappropriate manner. It wasn't one of our internal

systems but a system that we partner with another firm with that basically has that system.

The Chair: — So you're saying in three years you've had three incidences.

Mr. Norton: — The three that I'm aware of where people have accessed . . . again they had proper credentials but again accessing beyond what they were supposed to.

The Chair: — So in other words there was no . . . [inaudible] . . . criminal intent or even mischievous intent. It was just the rules weren't being followed to the T; is that what you're telling us?

Mr. Norton: — That's right. That's correct.

The Chair: — All right. The last question that I have before Ms. Crofford is also regards to the agencies coming onboard. How is that decided? Who decides who's coming on board? Maybe you don't even know. But is it a directive from Executive Council? Is it a directive from . . . or an independent decision made by different departments, or do you have a wish list, a sort of a priority list, and you go around and sell your services to the various departments? How does this happen that, you know, some of them came on as of September 30, 2005, others a year later, and some here are in the process now?

Mr. Wincherauk: — What we do on that is that we started this, I think it was July 2004. We had had success with a pilot project between the Department of Highways and Agriculture and the then deputy minister to the Premier was intrigued by this initiative and asked us to carry it out to the departments. It was never imposed on the departments.

We go in and do an extensive due diligence on each one of the departments about where their infrastructure is, what are the risks they're facing, all those type of things and then we present that to their executive and then their executive makes a decision to either join or not join the ITO. So far the cases, whenever we've presented it, has been compelling to the department and I think they see the benefits of consolidated IT organization.

And a lot of it revolves around that whole issue of, what do you do with security? In the old days you would have had 18 different departments attempting to deal with security, a lot of people managing security off the side of their desk. There weren't standards, there weren't processes. And at least we all have that in place right now.

And then the huge benefits that come from, you know, the fact that we can, our servers are now running, being fully utilized I think at around 80 to 90 per cent. In the old days we had tons of servers out there and they were only being utilized at around 45 per cent. So huge savings, lots of opportunities for the departments, but it's not imposed upon them.

The Chair: — What departments at the current time are not interested in your services?

Mr. Wincherauk: — I wouldn't say not interested. We're just bringing in Community Relations and Justice and Corrections, which are very huge. We have outstanding the Department of Labour, Saskatchewan Property Management, and the Department of Health. Those are the only three that I believe that are outside of our environment right now.

The Chair: — And do you do IT for Executive Council?

Mr. Wincherauk: — Yes, we do it for Executive Council and I think currently there are only two ministers' offices that are outside of our environment and that would be the two that relate to the Department of Health.

The Chair: — The two that relate to the Department of Health?

Mr. Wincherauk: — I think there's the Minister of Health and then I can't remember the name of the other. Minister Addley, Healthy Living.

The Chair: — Oh, I understand. Is there a reason why these are not . . .

Mr. Wincherauk: — I think it's just as we work on the due diligence with the Department of Health that will just follow its logical course.

The Chair: — And I also see that you're working with the Department of Environment. And this committee has had some very interesting discussions with the Department of Environment because there have been a fair amount of difficulties with administration policies and procedures. Does that culture provide problems for you? Are you the solution and the answer they've been looking for?

Mr. Wincherauk: — I think in the realm of IT it's been very useful to them. Our philosophy is that process is very good. You have problems when you have bad process. We bring good processes and a lot more rigour and discipline to what's gone on in the past. It's like having somebody change some of your applications. Well you've got to be able to justify it. You've got to be able to make a business case before we'll move forward on some of those, though. I believe, in our partnership, departments have clearly benefited from with working with us.

The Chair: — Thank you. Ms. Crofford.

Ms. Crofford: — Mine's more of a broad accountability question. When governments have technology systems like this, are you better off to move further in the direction of centralization in terms of authority and controls, or does a decentralized accountability system work better? And I mean the auditor can comment on this as well if you like.

Mr. Wincherauk: — Well I think it's a mistake to think of it as, as we have centralized we have acquired all the power and all the influence. That's not the case. The departments are more responsible than ever before. We have created in each organization that comes into our environment what we call an information technology management committee that sort of oversees the wants and the needs of that department. They then have to work it through our process to have decisions made on major application development.

And so it allows government to think more strategic now than ever before. Where in the past departments may have had the

resources and they would just go off and start some of these things, now they have to come back to . . . We have a business advisory committee that decides which initiatives should go first and there's a lot more coordination. And in the past where you'd have department A building a couple of things and then B would be building the same thing, we now try to have some enterprise coordination on that.

Ms. Crofford: — And is part of your role the integration of actual management information, for example, for Treasury Board and government or for outcome measures that the auditor talks about frequently? Is that part of the work you do with departments?

Mr. Wincherauk: — Yes.

Ms. Crofford: — Thank you.

The Chair: — Thank you very much. Sorry I was distracted here and it was my fault. Mr. D'Autremont, a quick question.

Mr. D'Autremont: — A couple of questions, yes, that I missed in my . . . When a department hasn't signed a service level agreement, how does the department then set its strategic directions or how does it measure the results of dealing with ITO?

Mr. Antunes: — So even though they don't have a signed service level agreement, as I said, we have a standard set of services that we provide that we basically say, here's what's in the standard service level agreement. And every month, once they get through integration, every month we start producing a report back to the department to say, on these key metrics here's how well we did this month, whether they're good or bad, and we have confidence intervals around those metrics. We provide that back to the department and they basically then can measure our performance on a monthly basis.

Mr. D'Autremont: — When you don't have a service agreement in place how are the costs distributed with the department? How is it determined who pays for what?

Mr. Antunes: — The department always pays for everything actually. It's one of the things about our service model is that we've left the budgets back in the departments. So they articulate to us what they're looking for for services and then we charge that back to them on a cost recovery basis.

Mr. D'Autremont: — So how, without a service agreement in place or even with a service agreement in place, how do the departments measure the value they're receiving from ITO?

Mr. Antunes: — So I guess a couple of things that we're doing around that. One is, I guess, as we go through the process, the due diligence analysis process, we give them a budget for the next couple of years so they get a sense of what it is they're going to be spending over the next couple of years. The decisions they make obviously influence, kind of, whether they want to do more application development or not will influence the costs. So that's one of the things that we're doing.

Another thing that we're doing is we've just recently released a request for proposal. We're going to have somebody come in and actually do an evaluation on us to see how well we compare today against other organizations of similar size and complexity and that type of thing, to benchmark ourselves. And we'll produce that information back, get a sense on where we stand, use it as a benchmark then for improvement.

And the other thing we do is we've done a couple of client surveys as well so we can go in and say okay — we did one, I think, last March, another one in December — so we can say, here's where we're at in terms of our services and how well they're changing and how our customers react to that. And then we can make changes in response to that.

Mr. D'Autremont: — Does that include cost factors as well, like monetary costs?

Mr. Antunes: — Benchmarking will include monetary cost factors as well, definitely.

Mr. D'Autremont: — Does the department have the opportunity to go out and get a tender or an evaluation of costs outside of ITO and compare that to the costs inside of ITO?

Mr. Antunes: — Once they've joined the partnership the agreement is, is that we will provide and manage all of the IT services, so any IT services that they need done will be managed by the ITO. And we use a combination of internal resources and private sector resources, so if there was a specific data application or a skill set that they require, we would go to the market to procure that service.

Mr. D'Autremont: — What's the confidence level from the departments that they're receiving the best value possible for that by going through ITO?

Mr. Antunes: — Well I think as you go through with a large organization there's economies of scale, so on some things there's definitely a better opportunity for them to save money and get savings because of the types of things that we can do. When we look at what we did with our desktops recently, where we entered into a long-term supply contract for 12,000 desktops, the type of prices that we're able to get because we're buying in such bulk, they would never be able to do as a department. Then when you start looking at other services around application development and that type of thing, I mean, it'd be as competitive as the marketplace because we would go through the standard SPM [Saskatchewan Property Management] processes for procurement.

Mr. D'Autremont: — Do they have the opportunity though to step outside of ITO to submit a possible tender for consideration, and through ITO?

Mr. Antunes: — Not at this time.

Mr. D'Autremont: — So they don't really . . . They have to take your assessments then that you have searched the marketplace and received the best cost available?

Mr. Antunes: — And we're bound by the government procurement policies to make sure that we are doing that. And I think the evaluation that we are going to be doing with this benchmarking firm will again provide some assurances that yes,

they are getting value for the investment that they're making.

Mr. D'Autremont: — The reports from the benchmarking firm, are those strictly for ITO and the department, or are they available to this committee?

Mr. Antunes: — We haven't started the project. We're just in the process right now of selecting the vendors. So the RFP [request for proposal] has been out, I think, for the last couple of weeks. We're just finalizing the vendor right now. But those would be available, yes.

Mr. D'Autremont: — I know I would be interested in them. I'm not sure if the committee would be interested in them, but I think it would show what value is being received by utilizing ITO versus other procurement measures.

Mr. Wincherauk: — I think that's exactly what we have to do. We have to go back and, you know, ask some questions: well is it working? How can we improve it, or what are we doing wrong? And where do you take these initiatives in the future? So it allows us to reflect back on. It also allows it . . . We believe it will support our case in the long run.

Mr. D'Autremont: — Okay. Thank you, Mr. Chairman.

The Chair: — Thank you for those two questions, Mr. D'Autremont. And if you have the information you could provide to the committee, perhaps you could cc the member from Cannington.

One more question then that I want to ask, and that is: is 100 per cent of your budget cost recovered from the departments, or is it a percentage of your budget that's cost recovered from the departments?

Mr. Wincherauk: — I think it's around 4 or 5 million which is our base budget, which is sort of for our corporate services, like the deputy ministers' offices, communications — those type of functions — but the rest of it is recovered from the departments.

The Chair: — Do you have a percentage or a number?

Mr. Antunes: — Yes. So our budget is around 4 to $5 million. We recover about $44 million from the departments. So . . .

Mr. Wincherauk: — And that will, I believe, will go up in this fiscal year to around $60 million.

The Chair: — So you're doing $60 million worth of business, but your budget shows up as 4 or 5 because the rest is all cost recovered.

Mr. Antunes: — That's right.

The Chair: — Okay. I understand. Thank you very much. Are there any further questions? I think I've learned a fair bit. This is fascinating stuff.

We have four recommendations to deal with. Are we ready to go to recommendations? Are you ready to go to recommendations? The first recommendation by the Provincial Auditor is on page 213. It reads:

> We recommend the Information Technology Office perform quality assurance tests to ensure its security policies and procedures are followed.

Do I have a motion? Ms. Crofford.

Ms. Crofford: — Mr. Chair, I'll move that we recommend concurrence and note progress on 1.

The Chair: — The motion is to concur and note progress. Is there discussion of the motion? Seeing none, we'll call the question. All in favour? It's carried unanimously.

Second recommendation is on page 214. It reads:

> We recommend the Information Technology Office follow its security policies and procedures.

Is there a motion? Ms. Crofford.

Ms. Crofford: — Yes. I think, Mr. Chair, till we get a little further down the line on this one, for now I'm going to just recommend concurrence.

The Chair: — All right. The motion is to concur with the recommendation. Is there discussion of the motion? Seeing none, we'll call the question. All in favour? Again that's carried unanimously. The third recommendation is on page 215. It reads:

> We recommend the Information Technology Office protect its systems and data from security threats.

Is there a motion? Ms. Crofford.

Ms. Crofford: — To concur and note progress.

The Chair: — A motion to concur and note progress. Is there discussion of the motion? Seeing none, we'll call the question. All in favour? Again I believe that's carried unanimously. The final recommendation is on page 216. It reads:

> We recommend the Information Technology Office have a disaster recovery plan for its data centre and client systems.

Is there a motion? Ms. Crofford.

Ms. Crofford: — And in an ever predictable fashion, I'll recommend that we concur and note progress.

The Chair: — Again a motion to concur and note progress. Is there discussion of the motion? Is there a discussion? Again seeing no discussion, then we will call the question. All in favour? And that's carried unanimously.

And that brings us to the conclusion of chapter 6. I want to thank you, Mr. Wincherauk, and your officials, for appearing before the committee and answering all the questions that were put to you, and wish you well in your future responsibilities of keeping track of all the information that flows through your machinery. I just happened to notice that you have your own Norton security system as well. I'll just throw that in for what

it's worth.

Committee members, we will not be meeting next week because of the Easter break. We will again meet on April 17 and the two chapters up for discussion will be on the Public Service Commission and First Nations and Métis Relations. I wish you all a blessed Easter and we will see you in a couple of weeks. I declare the meeting adjourned.

[The committee adjourned at 11:46.]