Fourth Session - Fortieth Legislature

of the

Legislative Assembly of Manitoba

Standing Committee
on
Public Accounts

Chairperson
Mr. Reg Helwer
Constituency of Brandon West

Vol. LXVII No. 3 - 2 p.m., Wednesday, February 25, 2015

ISSN 0713-9462

MANITOBA LEGISLATIVE ASSEMBLY
Fortieth Legislature

Member	Constituency	Political Affiliation
ALLAN, Nancy	St. Vital	NDP
ALLUM, James, Hon.	Fort Garry-Riverview	NDP
ALTEMEYER, Rob	Wolseley	NDP
ASHTON, Steve	Thompson	NDP
BJORNSON, Peter, Hon.	Gimli	NDP
BLADY, Sharon, Hon.	Kirkfield Park	NDP
BRAUN, Erna, Hon.	Rossmere	NDP
BRIESE, Stuart	Agassiz	PC
CALDWELL, Drew, Hon.	Brandon East	NDP
CHIEF, Kevin, Hon.	Point Douglas	NDP
CHOMIAK, Dave, Hon.	Kildonan	NDP
CROTHERS, Deanne, Hon.	St. James	NDP
CULLEN, Cliff	Spruce Woods	PC
DEWAR, Greg, Hon.	Selkirk	NDP
DRIEDGER, Myrna	Charleswood	PC
EICHLER, Ralph	Lakeside	PC
EWASKO, Wayne	Lac du Bonnet	PC
FRIESEN, Cameron	Morden-Winkler	PC
GAUDREAU, Dave	St. Norbert	NDP
GERRARD, Jon, Hon.	River Heights	Liberal
GOERTZEN, Kelvin	Steinbach	PC
GRAYDON, Cliff	Emerson	PC
HELWER, Reg	Brandon West	PC
HOWARD, Jennifer	Fort Rouge	NDP
IRVIN-ROSS, Kerri, Hon.	Fort Richmond	NDP
JHA, Bidhu	Radisson	NDP
KOSTYSHYN, Ron, Hon.	Swan River	NDP
LEMIEUX, Ron, Hon.	Dawson Trail	NDP
MACKINTOSH, Gord, Hon.	St. Johns	NDP
MALOWAY, Jim	Elmwood	NDP
MARCELINO, Flor, Hon.	Logan	NDP
MARCELINO, Ted	Tyndall Park	NDP
MARTIN, Shannon	Morris	PC
MELNICK, Christine	Riel	NDP
MITCHELSON, Bonnie	River East	PC
NEVAKSHONOFF, Tom	Interlake	NDP
OSWALD, Theresa	Seine River	NDP
PALLISTER, Brian	Fort Whyte	PC
PEDERSEN, Blaine	Midland	PC
PETTERSEN, Clarence	Flin Flon	NDP
PIWNIUK, Doyle	Arthur-Virden	PC
REID, Daryl, Hon.	Transcona	NDP
ROBINSON, Eric, Hon.	Kewatinook	NDP
RONDEAU, Jim	Assiniboia	NDP
ROWAT, Leanne	Riding Mountain	PC
SARAN, Mohinder	The Maples	NDP
SCHULER, Ron	St. Paul	PC
SELBY, Erin	Southdale	NDP
SELINGER, Greg, Hon.	St. Boniface	NDP
SMOOK, Dennis	La Verendrye	PC
STEFANSON, Heather	Tuxedo	PC
STRUTHERS, Stan	Dauphin	NDP
SWAN, Andrew	Minto	NDP
WIEBE, Matt	Concordia	NDP
WIGHT, Melanie, Hon.	Burrows	NDP
WISHART, Ian	Portage la Prairie	PC
Vacant	The Pas	

LEGISLATIVE ASSEMBLY OF MANITOBA

THE STANDING COMMITTEE ON PUBLIC ACCOUNTS

Wednesday, February 25, 2015

TIME – 2 p.m.

LOCATION – Winnipeg, Manitoba

CHAIRPERSON – Mr. Reg Helwer (Brandon West)

VICE-CHAIRPERSON – Mr. Matt Wiebe (Concordia)

ATTENDANCE – 11 QUORUM – 6

Members of the Committee present:

Hon. Messrs. Dewar, Gerrard

Messrs. Friesen, Gaudreau, Helwer, Jha, Maloway, Marcelino, Pedersen, Schuler, Wiebe

Substitutions:

Mr. Gaudreau

APPEARING:

Mr. Ralph Eichler, MLA for Lakeside
Mrs. Heather Stefanson, MLA for Tuxedo
Mr. Norm Ricard, Acting Auditor General
Mr. Doug Harold, Principal, Office of the Auditor General

WITNESSES:

Hon. Mr. Robinson, Minister responsible for Manitoba Hydro
Mr. Scott Thomson, President and Chief Executive Officer, Manitoba Hydro
Mr. Bryan Luce, Vice-President, Human Resources and Corporate Services, Manitoba Hydro
Mr. Glen Reitmeier, Division Manager, Information Technology Services, Manitoba Hydro

MATTERS UNDER CONSIDERATION:

Auditor General's Report–Annual Report to the Legislature, dated March 2014

Chapter 8–Managing Cyber Security Risk Related to Industrial Control Systems

* * *

Mr. Chairperson: Good afternoon. Will the Standing Committee on Public Accounts please come to order.

This meeting has been called to consider Chapter 8–Managing Cyber Security Risk Related to Industrial Control Systems of the Auditor General's Report–Annual Report to the Legislature, dated March 2014.

Pursuant to our rule 85(2), I would like to inform the committee that Mr. Gaudreau will be sitting in for today's meeting.

Are there any suggestions from the committee as to how long we should sit this afternoon?

Mr. Blaine Pedersen (Midland): Mr. Chairman, our normal practice is to sit for a couple hours. So I would suggest we sit for two hours unless we finish sooner, and if we're not, reassess at that time.

Mr. Chairperson: Is that the will of the committee? *[Agreed]*

I see the minister and the CEO of Hydro are at the table, so welcome. And, if you have an opening statement and if you'd like to introduce any staff that are with you, please.

Hon. Eric Robinson (Minister responsible for Manitoba Hydro): Of course, I'm with Mr. Scott Thomson, the president and CEO of Manitoba Hydro and after a few remarks that I have to make, he'll be introducing the staff that have accompanied him to this committee this afternoon.

First of all, I want to thank the committee for allowing us to discuss some issues relating to the report that has been tabled by the Office of the Auditor General, and as you know, the Office of the Auditor General Report, Chapter 8, Managing Cyber Security Risk Related to Industrial Control Systems. Manitoba Hydro takes this issue very seriously and is committed to addressing the recommendations that are identified.

And I want to highlight for this committee the modern industrial control systems, the use of computers and software that control devices used for generation, transmission and distribution of electricity and natural gas. Over time the systems have evolved into the functionality from basic mechanical controls to more sophisticated software systems along with the increased functionality of the associated cybersecurity risks have been–have increased as well over time. It's important to note that industrial control systems security risks are separate from traditional information technology systems and security. Manitoba Hydro is confident that steps are in place to effectively secure systems containing sensitive customer or commercial information. In addition, Manitoba Hydro's two most critical facilities related to bulk power, the system control centre and the backup system control centre, are secure, both from physical and cybersecurity from the–from both the physical and cybersecurity perspectives.

From an overall risk management perspective, Manitoba Hydro manages risk through the Corporate Risk Management Steering Committee and submits an annual report to the Manitoba Hydro-Electric Board. As of November 2014, the Corporate Risk Management Report includes cybersecurity as a new and separate corporate risk profile. The Audit Committee of the Manitoba Hydro Board has also received two progress reports regarding the Office of the Auditor General's recommendations. A new governance model has been put in place at Manitoba Hydro regarding security. The Enterprise Security Council comprises of Manitoba Hydro's executive and chaired by the vice-president of Human Resources and Corporate Services. It also provides executive oversight relating to all corporate security functions, develops and executes strategy, sets priorities and provides governance relating to security policy. The Enterprise Security Council also provides oversight to ensure security advisory committees regarding physical sensitivity, technology security and regulatory compliance.

As I noted at the outset, the Auditor General has provided eight recommendations, and all eight of these recommendations have been received by Manitoba Hydro and all eight recommendations are being addressed in one fashion or another, and I'm sure that Mr. Thomson will get into more details about how they're being addressed.

So, with that, I'd like to turn the floor over to Mr. Thomson who will provide further background information and the status that Manitoba's hydro–Manitoba Hydro's work towards the implementation of the recommendations contained in the office of the Auditor General's report. While Manitoba Hydro recognizes they have work yet to do in this area, I commend them for the attention they have paid to this important topic and the efforts that they've extended on this initiative thus far.

Mr. Chairperson: Thank you, Minister Robinson.

Before we go to you, Mr. Thomson, I'll ask the acting Auditor General for his opening statements.

Mr. Norm Ricard (Acting Auditor General): Before I do my opening statements, I would like to introduce the staff member that I have with me today, and that's Doug Harold. Doug Harold is an IT audit principal in the office who specializes in cybersecurity. He's also the principal who conducted this audit. I'm pleased to make him available to the committee today to answer any questions you may have that are of a more technical nature.

Mr. Chair, cyberattacks have increased dramatically in the past few years. Recent attacks we are no doubt all familiar with occurred at Sony, at Home Depot and Target. Whether the–a specifically targeted attack or simply a random, opportunistic attack, governments and businesses must properly assess cybersecurity risks and implement effective controls. Unfortunately, these threats are often underplayed.

In this audit we wanted to assess how vulnerable Manitoba Hydro was to cyberattacks. We looked at whether Manitoba Hydro's risk management practices relating to its industrial control systems reasonably mitigated cyber risks. Manitoba Hydro uses many industrial control systems to monitor and control generation, transmission and distribution of electricity as well as the distribution of natural gas. The consequences of a cyberattack on its industrial control systems could be significant because the entire electric system could be affected, potentially disrupting the flow of electricity, causing significant risk to the health and safety of Manitobans.

In 2003 Manitoba Hydro–since 2003 Manitoba Hydro has been working towards complying with the reliability standards of the North American Electric Reliability Corporation, including its cybersecurity standard. The North American Electric Reliability Corporation, commonly referred to as NERC, is an international regulatory authority established to reduce the risks to the reliability of the bulk electric system in North America.

But compliance to the cybersecurity standards–but compliance to its cybersecurity standards focuses on assets critical to the bulk electric system rather than to Manitoba Hydro's overall operations. So, for NERC compliance purposes, only two physical locations have been identified as housing critical cyber systems which must be protected using these standards. These systems do not necessarily represent the only control systems that are critical to add to the hydro operations. NERC's standards and Manitoba Hydro's related compliance efforts should not be interpreted as adequate corporate cyber-security risk management. Simply put, compliance does not equal good security.

***** (14:10)

We found that Manitoba Hydro had not prioritized its industrial control systems and related IT systems for criticality to its generating, transmitting and distributing processes. In addition, while their risk management process includes 52 risk profiles, industrial control systems cybersecurity risk is not among them. As such, these risks have not been communicated to the board. Without comprehensive and co-ordinated industrial control systems cybersecurity risk assessments, Manitoba Hydro may not be able to design and implement effective security controls for its systems.

So we visited six locations being four generating stations, a modernized transmission substation and a high-voltage direct current converter station. Each one of these locations makes use of industrial control systems that we believe are critical to Manitoba Hydro operations, but they were not NERC critical assets. We compared the cybersecurity practices in place at these sites to Public Safety Canada's recommended best practices for industrial control systems. These are the minimum standards that should be implemented by all industries that use industrial control systems.

While some security controls were evident at each location, we identified serious weaknesses in cybersecurity controls. Our report notes several factors that we believe have led to this lack of attention to cybersecurity risks. These include: a false sense of security about the effectiveness of the existing configuration and a focus on NERC compliance; no executive with responsibility for corporate-wide cybersecurity or for corporate-wide physical security; no comprehensive industrial control systems cybersecurity policies; and no industrial control systems security awareness program and training.

Mr. Chair, we concluded that cybersecurity risks related to industrial control systems were not being identified, assessed and managed. Until Manitoba Hydro has assessed the risks to all of its industrial control systems, it cannot be certain that it has applied the appropriate level of controls to prevent unauthorized access, modification or damage to these vitally important systems. This leaves them vulnerable to a cyberattack that could lead to significant consequences for the province.

This report includes eight recommendations, and we will be following up on the implementation status of the recommendations as of June 30th, 2015.

Thank you, Mr. Chair.

Mr. Chairperson: Thank you, Mr. Ricard.

And welcome, Mr. Harold. We welcome your expertise to the committee.

Now, the president and CEO of Manitoba Hydro, Mr. Thomson. I believe you have an opening statement, sir. And would you introduce any staff that you brought with you, please.

Mr. Scott Thomson (President and Chief Executive Officer, Manitoba Hydro): Good afternoon, Mr. Chair, committee members.

I'd like to thank the members of the Public Accounts Committee for this opportunity to provide remarks on the Auditor General's report, chapter 8. And before I begin, as indicated, I'd like to introduce the staff that are here with me today: Bryan Luce–maybe you can just acknowledge yourself, Bryan–is our vice-president of human resources and corporate services, and he's responsible for both physical and IT security amongst other things; Glen Reitmeier –Glen's a division manager of Information Technology Services, and he reports directly to Bryan and is responsible for IT security. And Glen is joined here today by one of his managers, Rob Lanyon, who is leader of the Office of the Auditor General program, which I'll describe in more detail as we move forward.

As you know, the objective of the Auditor General's review was to determine whether Manitoba Hydro's risk management practices ensure the design of security controls over industrial control systems and related information technology in that it reasonably mitigates identified cyber risks. The OAG concluded that the cybersecurity risks related to ICS systems are not identified, assessed and managed. Eight recommendations were made in the report to address these concerns, and I'd like to thank the Auditor General for raising these items to the attention of Manitoba Hydro. We weren't caught completely unaware; work had been under way. I did–I want to assure the committee that this wasn't–you know, didn't catch us flat-footed.

As described in the OAG report, industrial control systems have evolved in functionality from basic mechanical controls to more sophisticated software systems, including the ability to connect to information networks. Along with the efficiencies gained through these advances, the associated cyber risk has also increased. It's important to note that the industrial control systems under discussion are separate from what we would describe as corporate IT systems and IT security. Manitoba Hydro's experience in securing IT systems is extensive, going back over 30 years. Our experience related to ICS security is relatively new, dating back to our first NERC reliability compliance efforts which, as had previously been indicated, concentrated on our most critical industrial control system, the transmission control centre.

I'll now provide comments on Hydro's overall progress regarding cybersecurity for industrial control systems and give a brief update on each of the recommendations contained in the report.

Overall, I can assure the committee that Hydro has taken these recommendations very seriously. Prior to the former release of the OAG report, Manitoba Hydro immediately established a corporate security council to govern corporate security. Following the release of the OAG report, the council was renamed the Enterprise Security Council. The governance model now in place regarding physical security, technology security, and NERC compliance consists of the Enterprise Security Council, the technology security advisory committee, the physical security advisory committee, and the NERC reliability compliance steering committee.

The Enterprise Security Council subsequently approved the creation of the–of what we're calling the OAG program, which is a series of projects that share the common goal of improving the physical and technology security related to ICS at Manitoba Hydro and specifically focused on the recommendations made in the OAG report.

One of the first steps taken by the OAG program was to seek out and engage a recognized ICS security–cybersecurity consulting firm to assist with our efforts. The consulting firm established during the engagement that our current state of–regarding ICS cybersecurity is typical amongst Canadian utilities. Notwithstanding that, we recognized that a more formal approach was needed.

The engagement was successfully completed and has provided foundational components to address ICS cybersecurity risks. This was a critical first step to tackle the complex task of identifying and assessing all critical ICS assets across Manitoba Hydro's substantial infrastructure. A high-level strategy has been created to improve the cyber-security posture of industrial control systems at Manitoba Hydro. This ICS security strategy outlines a long-term plan for ICS security program development, risk management framework implementation and security controls and monitoring capabilities. It's the foundation for ongoing ICS security improvement projects and plans which drive and demonstrate continuous improvement for ICS security going forward. This represents a significant effort for Manitoba Hydro that will be achieved through short- and long-term initiatives. Building upon these initial steps, Manitoba Hydro is now in a position to execute this strategy involving several projects that will improve our cybersecurity posture.

I'll now provide an update for each OAG recommendation.

As it relates to recommendation 1, which was identify, assess, and mitigate all ICS cybersecurity risks, that this be performed on a priority basis for assets critical to operations, so drawing your attention to recommendation 1, this effort is the most significant in terms of full implementation. Achieving identification, assessment and mitigation of all ICS assets requires establishing an ongoing methodology supported by industry standards and best practices. Recognizing that this effort is a continuous activity and the number of assets in scope is extensive, the work is broken down into several components and phases.

The progress to date has followed on the following three areas: First, identify high-priority asset locations. A list of physical locations that are most critical to Manitoba Hydro operations has been created. The list provides an initial priority for identification and assessment activities that will take place in the risk management framework project which I will describe next.

A consulting engagement with a firm specializing in ICS security was completed in December of this past year. The main deliverables are an ICS security risk management framework and a high-level implementation strategy. These are foundational components I referenced earlier. These deliverables were presented and approved by the technology security advisory committee and the Enterprise Security Council.

Project planning is under way to implement the risk management framework beginning next month. The same consulting firm will be engaged to assist Manitoba Hydro in developing ICS policies and the implementation of those policies on critical ICS assets. The engagement will create a repeatable process that Manitoba Hydro can use to carry forward a self-sustaining ICS cybersecurity risk assessment program.

***** (14:20)

Thirdly, physical security: A project to deploy a centralized security management system at the transmission system control centre and the backup control centre was endorsed by the physical security advisory committee and approved by the Enterprise Security Council. The system will form part of the solution to mitigate ICS physical security risks. Further development will be planned following the first phase and done according to the high-priority asset location 'lisk'–list and the NERC CIP version 5 compliance requirements–and I'm going to need a glass of water.

The second recommendation was, once cybersecurity risks have been identified, include cybersecurity as a corporate risk profile in the annual risk management report that is presented to the board. Regarding this recommendation, the November 2014 Corporate Risk Management Report did include a cyber–includes cybersecurity as a new and separate corporate risk profile. The implementation of the risk management framework described above will provide processes to update the risk profile each year. So we consider this recommendation to have been implemented.

Third recommendation, assign responsibility for corporate-wide cybersecurity to one executive, and the related item 5, assigning responsibility for corporate-wide physical security to one executive. All technology and physical security responsibility now reports functionally to Bryan Luce, our vice-president, Human Resources and Corporate Services.

As I earlier indicated, the governance model of security committees is in place, terms of reference for all committees have been approved, and meetings are ongoing on a quarterly basis or more frequently as required. We consider these recommendations also to have been implemented.

Recommendations 4 and 6 will also be addressed together. These recommendations will be achieved through a policy development project reporting to the technology security advisory committee. The project will incorporate the policy recommendations made by the Auditor General for both physical and cyber controls, a review and restructuring of all existing IT policies and an update of NERC policies related to CIP version 5 compliance. A security firm specializing in policy writing will be engaged to assist with this project beginning next month as well.

Recommendation No. 7, which was to develop and deliver a comprehensive ICS cybersecurity training and awareness program for all staff responsible for the operation, maintenance and security of ICS systems. The scope of this project is to develop or procure and deliver an ICS cybersecurity training program for staff responsible for the stated objectives. Much like the policy development project, it is our intention to also include IT security, physical security and NERC training modules to ensure co-ordination of effort and consistent delivery to employees. This project is scheduled to follow the policy development and the risk management framework projects contained in recommendations 1 and 4.

Finally, recommendation 8, which was to develop a strategy to converge IT and OT management, including IT security. The scope for this recommendation is to develop a strategy to converge these areas and contain several initiatives and projects that are related to operational efficiencies, ICS cybersecurity best practices or NERC CIP 5 compliance. For example, an enterprise patch management system project comprised of an enterprise IT and ICS patch notification service and patch management systems has been initiated. IT security is involved in the development of the proposed strategy. We anticipate this recommendation to be implemented when the technology security advisory committee and the Enterprise Security Council approve the strategy document.

In closing, although Manitoba Hydro is pleased with the progress made over a relatively short period of time since we received the report in March of last year, a substantial effort still lies ahead to fully implement all of the recommendations, recommendation No. 1 in particular. Securing all of our ICS assets and establishing the process to maintain that security is, simply put, a lot of complex work requiring substantial human and financial resources. Fully achieving our ICS cybersecurity objectives is a long-term project, and we're not alone, as I'd indicated earlier. The industry as a whole across North America is facing the same types of issues.

To summarize our progress, then, several important foundational steps in securing our ICS assets and implementing the OAG recommendations have been achieved over the past 12 months. These include: established the enterprise-wide security governance, created the OAG program, identified and ranked our most critical asset locations. We've drafted an IT-OT management strategy. We've identified and organized the subject matter expert employees currently implementing cybersecurity for ICS, raised awareness throughout the organization through internal articles and other communications. We've co-ordinated security activities between IT, OT, NERC and physical staff security, initiated a centralized security management system regarding a standard, centrally managed physical security access control and monitoring, and planned and readied for execution the policy development project, the risk management framework project and the training and awareness project.

That concludes my opening statement. Thanks for your attention and I'd be happy to answer any questions you might have.

Mr. Chairperson: All right, thank you, Mr. Thomson.

Before we get into questions, I'd like to inform those who are new to this committee of the process that is undertaken with regards to outstanding questions. At the end of every meeting, the research officer reviews the Hansard for any outstanding questions that the witness commits to provide an answer and will draft a questions-pending-response document to send to the witness. Upon receipt of the answers to those questions, the research officer then forwards the responses to every PAC member and to every other member recorded as attending that meeting. At the next PAC meeting, the Chair tables the responses for the record.

Now, one last item, I would like to remind members that questions of an administrative nature are placed to the witness, Mr. Thomson, the CEO, and that policy questions will not be entertained and are better left for another forum. However, if there is a question that borders on policy and the minister would like to answer that question or the witness wishes to defer it to the minister to respond to, then that is something we would consider.

The floor is now open for questions.

Mr. Ralph Eichler (Lakeside): Yes, thank you for your opening comments. I do have a couple of questions in regards to your opening statement. On page 4 you talk about a security firm specialized in policy writing will be engaged to assist with this project beginning in March of 2015. Would you highlight how you went about securing this firm and the process that was developed to seek out this firm, and is it a local firm?

Mr. Thomson: Can I–can–I'm just wondering how I might be able to use my support staff.

Mr. Chairperson: You can certainly confer with staff. You can bring them up beside you at the table, if you wish, and we can get a chair there for you.

Sorry, before we go ahead, Mr. Thomson, if you're going to have one of your staff answer the question, then we'll have to introduce them to the record or he can confer with you and you can answer, whichever way you wish, but you can introduce him to answer the question if you wish.

Mr. Thomson: If I might, on this question I'll ask Mr. Luce to address the committee.

Mr. Chairperson: Sorry, Mr.–

Mr. Thomson: Bryan Luce.

Mr. Chairperson: Mr. Luce. Okay, Mr. Luce.

Mr. Bryan Luce (Vice-President, Human Resources and Corporate Services, Manitoba Hydro): We've engaged two security firms–

Mr. Chairperson: It's probably best if you sit to–so that the microphone can pick up your voice because this is being recorded for Hansard and then we'll be able to hear you. Thank you, Mr. Luce.

Mr. Luce: We engaged two security firms over the last 12 months to assist the organization in identifying, first of all, a risk methodology to assess our ICS security risk, as well as another firm to assist us on our IT policy development. We found that, as we were looking in terms of the selection of these particular firms, we found that the cybersecurity space in terms of IT consulting is very new and emerging within at least Canada, from our perspective, when we did a search for a consultant.

***** (14:30)

And we identified a consultant out of Vancouver that seemed to be one of the industry experts in Canada through our association with the CEA and participating utilities within that particular forum, and essentially sole-sourced that particular engagement to that specific consultant because they're very few and far between. So that would be the first one, and the second one we did initially in relation to doing an ITS security audit, called for proposals through a request for proposal in which we selected this particular firm to do the ITS security audit, and then subsequent to that we've engaged them, based on the work that they did for us, on a separate engagement, if you will, through a sole-source as well.

Mr. Eichler: For the record, could we have the names of those firms? And what basis is the expenditure calculated as far as cost is concerned?

Mr. Luce: So, Lofty Perch would be the one from out of Vancouver that we've used. And did you ask the cost of the initial engagement? I believe the–that initial engagement in terms of the risk-assessment methodology was $100,000.

Mr. Eichler: In regards to your cost analysis based on what you submit to the PUB, are these costs in that calculation that you recently presented to the PUB based on your rate increase?

Mr. Luce: I don't believe they are. These are relatively new estimates and costs in relation to the work that we've done to date.

Mr. Eichler: Based on your initial presentation, then, what is the amount of money you're expecting to expend for the security that you're basing them on, at this point anyway?

Mr. Luce: It's difficult to anticipate that. I can give you a sense as to what we've spent so far since we've proceeded with this particular project–and that would've been about a year ago about now–in and around $2.8 million to date. A lot of that would include staff time, implementation of the central monitoring system that we had talked about.

It's difficult to forecast what the actual cost is because we're talking about–just the order of magnitude, talking about applying a risk methodology to some 130 critical sites. And until we apply that methodology to those sites, we will not have a good sense as to the degree of risk that exists within those sites and what our mitigation plan might be to mitigate the risk that we do find out. So I think that it's fair to say that we're talking about millions of dollars.

Mr. Eichler: The security firm, is it overlooked by your–any of your security advisory committees? And, if so, what role do they play? *[interjection]*

Mr. Chairperson: Mr. Luce, I have to identify you so that Hansard recognizes who is speaking. So, Mr. Luce.

Mr. Luce: Fair enough.

The Enterprise Security Council plays a very important role in terms of providing guidance in overall conduct of the program, first of all, across the corporation, but specifically in relation to the consultants that we've engaged. As an example, December of last year, a Lofty Perch was in to provide us with their recommendations on risk-assessment methodology for the next phase of work on this. That was presented to the Enterprise Security Council and endorsed by the council.

The actual work that they will now do in relation to helping us with this risk methodology will be under the guise of the Enterprise Security Council in terms of providing conduct, in terms of providing oversight and direction under the guise of the Enterprise Security Council and the technology security advisory committee. They're very, very tightly integrated.

Mr. Eichler: The committee that's established–and obviously you have a number of those committees–how is those committees made up? Is it in-house or are they hired or are they consultants that's been 'pecifically' hired for this update, and if you'd outline that for us.

Mr. Luce: The Enterprise Security Council–I'll start with that first of all–that's a council that I chair that's made up of senior vice-presidents across the organization that have operational responsibility. Whether it's customer service and distribution, transmission or generation operations, that comprises that particular committee.

The advisory committees are again subject-matter experts from within Manitoba Hydro that would chair each of the respective committees. By way of example, the technology security committee is chaired by Mr. Glen Reitmeier, who is the senior manager for IT technology within Manitoba Hydro, and his committee is comprised of representatives from across the organization who are impacted by the particular review that we're undertaking. And that goes the same for the physical security committee, is led by my division manager of corporate services who has responsibility for physical security within the organization and similarly on the NERC side. So they're all internal resources to Hydro.

Mr. Eichler: So based upon these various committees you've established to dwell into the policy and so on, what is the anticipated timeline before you seek to where you're going to be comfortable with the recommendations been brought forward and the timeline you established to try and implement those and have them finished?

Mr. Luce: The largest piece of work in relation to working to mitigate our risk has to do with applying the risk methodology that we've talked about onto our 130 locations or so; that's a massive undertaking.

Our plan this year is to try and work through five of the most critical sites as we start this initiative in terms of applying that methodology against those sites.

So, to be honest and to be fair about this, this is–in our mind this could be a five-, six-, seven-, eight-year project; it's a long-term project. But our focus, of course, is on those mission critical priority locations to start with.

Mr. Eichler: So taking it to the next step for prevention down the road, what is the–is this committee then going to be responsible for any other issues that may come forward? So this will be an ongoing committee. Looking in, once you get those recommendations implemented and approved and feel secure about it, those next steps, what would they look like?

Mr. Luce: So we set up this Enterprise Security Council governance model, is not a project but an actual way in which we're doing business going forward. So there isn't an end to this in our mind. We have the OAG issues to deal with, but we also have a variety of other issues to deal with that might be IT related or physical security based. So this is a permanent function or fixture within our organization; it's not a project.

Mr. Ron Schuler (St. Paul): One very short question: Has Manitoba Hydro ever come under a cybersecurity attack?

Mr. Luce: I would not say we have come under a cybersecurity attack to the best of my knowledge, but I am aware of one incident where we did have an issue, and, perhaps, if I can, ask Mr. Reitmeier to respond to the details around that.

Mr. Chairperson: Sure, if you wish.

Mr. Glen Reitmeier (Division Manager, Information Technology Services, Manitoba Hydro): Yes, this July at the Riel transmission station we had our one and only incident–industrial control incident–reported.

There's a station automation system. It's our new–a new transmission station, and in there's a system called a station automation system and it has a local network that isn't connected to any other corporate networks and it controls the station.

In July the staff started noticing that it was not–that the system wasn't acting properly; there were some performance issues with it, and after a security investigation it was found out that there was a worm on the–one of the servers. So that's a virus, and an outage for the station automation system had to be taken out for approximately, I think it was, eight hours. The station itself was still in service, was still performing, but the control system for the station had to be taken out for eight hours to get rid of the virus and bring the system back to normal conditions. That's the only incident we've had and it did not end up taking out the power system or any piece of it.

Mr. Cameron Friesen (Morden-Winkler): Thank you for that answer. Still on that same subject, I would understand that, within the corporation and probably after an event of that magnitude or that seriousness, there would be an examination as to what had occurred and what would have been the, you know, the cause of that.

What was it that Hydro determined would have led to such a–the insertion of that kind of a, you know, malevolent software into the system?

***** (14:40)

Floor Comment: The–

Mr. Chairperson: Mr. Reitmeier.

Mr. Reitmeier: Sorry. The cause wasn't precisely determined, but it would have been brought in either with a technician connecting a PC to the station automation system or through a USB, you know, flash key, or possibly it came with the virus from the manufacturer. We're not sure which one of those three, but it was not introduced through a network; it was introduced through some sort of manual working on the system.

Mr. Friesen: I'm interested in that response because I know this was an area that the Auditor General's office had cited as being an area that, in their examination, that there were vulnerabilities. And I believe that the report, actually, in chapter 8, described exactly this type of scenario whereby–I mean, we understand we're not the professionals in this area, but we understand how operational technology has become increasingly, you know, it's become increasingly a technological thing; it looks like IT–OT and IT, the line becomes increasingly smaller.

So I guess I'm wondering, from an operational perspective, then, and I understand these things are tremendously complex, how does Hydro, then, respond? How do they make the system safer? If they're going to do a post-event analysis and say, all right, we've got to be very careful about USB; we have to be very careful about laptops coming in with technicians to these stations, how does that analysis take place, and is that an analysis that now would take place under one of the new committees or entities being formed by Hydro?

Mr. Reitmeier: I think that, you know, that's a very good question, and, you know, when you look back at what the OAG has recommended, we have processes missing with our industrial control systems. And so we have this–we don't have a risk assessment methodology in place. That's what we're putting in right now, and then we're going to be going to assess the assets, and that will list all the vulnerabilities. Then we'll have to determine which ones have to be mitigated and which ones we would accept for a risk.

So our long-term plan is to put all that in place, and when this–an incident like this would be–would occur, it would be immediately addressed with this whole risk assessment and mitigation process that we're putting in place. In the interim, we're going to have this gap where incidents happen. But they're so infrequent; we've had one. It's–we have quarterly newsletters that we put across the organization. We have meetings with focus groups. Our IT security department makes presentations to–somewhere between 12 and 20 a year to various departments.

So, you know, we're communicating that it's not only technology; it's people and process that create these cybersecurity issues. So it's a lot a communications that we're trying to build on. So we're going to have this period of time; until we actually implement this methodology that we're building, we're going to be still in a manual mode, if you will.

Mr. Friesen: I thank you for that answer. Earlier this afternoon, Mr. Luce had said that, of course, the focus is on the priority assets, and I would imagine, then, the idea would be we're going to identify the priority assets and work down to eventually be able to have a comprehensive system that analyzes the risks at all of these assets belonging to Hydro. My question for you is: Would this–where the incident took place, would that have been a priority asset for Hydro? Or where would that have ranked in the scale of priority assets?

Mr. Reitmeier: It would have ranked No. 4.

Mr. Chairperson: Sorry, Mr. Friesen.

Mr. Friesen: So it's a No. 4 priority. How many priority levels would there be within the corporate–

Floor Comment: We just have them ranked–

Mr. Chairperson: Mr. Reitmeier.

Mr. Reitmeier: Sorry.

Mr. Chairperson: It's okay. Go ahead.

Mr. Reitmeier: We have them ranked from one to 140. So some are tied, and so there aren't different levels; they're just–they're all ranked.

Mr. Chairperson: Mr. Thomson, you had a response as well?

Mr. Thomson: Yes, I just wanted to interject that it's not that there are different levels of priority ranking *[inaudible]* But the higher ranked items would be things like our control centre, our stations, you know, that–those key assets in the system. So Riel, being a new station, it would be one of the higher ranking assets in the system. It's not like we tier them per se.

Mr. Friesen: And I appreciate that clarification, but just for further clarification, just so I can understand how this comprehensive analysis will take place within the corporation, I know that at one point in the OAG chapter they actually referred to the number of separate assets that Hydro considers–and I know there were only two of those under the study that were determined to be, like, risks in this way to cybersecurity.

So do I understand correctly that this analysis will eventually take place considering hundreds of separate assets belonging to Hydro, however they compartmentalize those? Take a transmission line and divide it into segments, I would assume, or something like that. How many assets, I guess the question is, would actually be under consideration for this comprehensive study?

Mr. Chairperson: Mr. Luce–or Mr. Reitmeier, you have the–*[interjection]* Sorry, go ahead.

Mr. Reitmeier: We don't know the answer to that question until you get into an asset location. We are currently, and as part of our NERC compliance project, inventorying 13 of the highest critical sites, asset locations. So we'll have a better idea–we're piloting–we're going into five first and that's going to give us a better idea as to how much–how many assets will be in different types of sites. So there could be, yes, hundreds of assets that need to be looked at, depending on the complexity of the site and how new it is.

Mr. Luce: Yes, just to top up on that a little bit, we're talking about potentially hundreds of assets within a location. I just wanted to provide that clarification. We've identified in and around 130 high-priority locations, but within each location there's a large, large number of various assets *[inaudible]* we can look at. So that's why we developed this risk methodology, to be able to identify what's an acceptable level of risk, where do we need to pay our attention on, because this is, like I said, a massive undertaking.

Mr. Chairperson: Mr. Thomson, I'm not sure if you want to take this one, I do have a bit of a question on this, or one of your staff may.

But Hydro has long had a culture of safety. I mean, it's denigrated by some of its staff because they have to do certain things, but it's certainly celebrated and the linemen and the managers that I talk to, it's throughout the organization. Now you're having to add to this a culture of security. So you talked a little bit about the things you've done to try to bring some of that in, but in the culture of security, like safety, people think it'll never happen to them, you know, my computer's safe so I can come and bring it to work and connect it to the network, it'll be fine, nothing will ever happen.

So how do you expect, if you can give us a guideline of the process, to move to that culture of security that you need throughout Hydro?

Mr. Thomson: Yes, I think one of the key areas that we'd indicated was in and around communications and education with staff. It will become and is becoming already an element of that training and awareness program around these things, and the endgame to that is so that it's just as part of the culture as safety is part of the culture.

We operate a critical system for the province and, again, as indicated, there's so far–and hopefully we'll be able to limit it to that–one incident that has occurred. It didn't actually interrupt the flow of power and we were able to use backup and manual systems behind it.

***** (14:50)

But we have to be vigilant and we can't let our guard down, and this is evolving and it will continue to evolve. So it will be part–become part of the fabric of the organization as well.

Mr. Chairperson: Mr. Eichler–oh, Mr. Luce, did you have another addition there? You can–it'll pick it up. You don't have to move the microphone, because otherwise when you set it up and pick it down, they hear it in their headsets.

Mr. Luce: Okay, that's what the funny looks are for.

Mr. Chairperson: That's right, yes. So–

Mr. Luce: Just to top up on that again, and I want to make the distinction between what I would call our enterprise IT systems and the operating technology or industrial control systems within, let's call it the hundred and thirty, forty sites that we've talked about. Because I believe that there is–it would be my opinion that there is a culture of security when it comes to enterprise IT. As Mr. Thomson's statement alluded, that when you think about our enterprise IT systems whether they're financial, whether they're customer-based, whether they're billing systems, proprietary information, we've got good security practice and protocol around that and we've been auditing those for years and making improvements as a result of audits.

So I just want to, again, make that distinction between that and these industrial control systems which are essentially an emerging threat, if you will, relative to our business.

Mr. Eichler: I want to come back to your opening comments, Mr. Thomson. In regards to page 5 you had made reference to the ICS cybersecurity best practices or the NERC CIP version 5 compliance. Could you just go into a little bit more detail on what your goal is there and how you'd want to try to achieve it?

Mr. Thomson: Yes. I'm going to–for the version 5 piece, I'm going to have to confer with my colleagues here.

Mr. Chairperson: Mr. Thomson, you can have someone else answer if you wish, but feel free to confer.

Mr. Luce: Can I ask you to repeat the question just to make sure that we're on the right section here?

Mr. Eichler: Sure. In their comments there was talk about the ICS cybersecurity best practices, or the NERC CIP version 5 compliance. My question was, what does that entail and what's the timeline and how are you going to get there based upon the statement that you made?

Mr. Reitmeier: So the tactical group that's responsible for–going to be responsible for ICS security is addressing not only the OAG recommendations but this NERC compliance that is extending from our two control centres to locate 16 sites within the next 15 months, and so we're trying to co-ordinate all our activities so that we're not trying to duplicate tasks when we meet one set of standards and also meet the office of the Auditor General recommendations, which really is security best practices.

So we have a group that had started working even before the OAG report that was looking to see at Manitoba Hydro how, what we call corporate IT world, could help the industrial control systems, and this was starting–a project that started to see if tools that were used in that world could help the industrial control systems. That working group were successful in making that conclusion, and that working group consisted of the different industrial control operating support people in the organization and they came up with some recommendations to develop an IT-OT convergence strategy. And what's in that strategy is, first of all, the theme as security should be centralized, and there's some responsibilities. The business, these industrial control areas, support areas, would like corporate ID to provide them with the patches, the notifications in how to update their industrial control systems. The responsibility's been defined for the business unit areas. They are still responsible, the industrial–you know, these industrial control support areas–they have to implement tests that implement. So we're defining in the strategy responsibilities for IT and for the business, and then within that strategy it's initiating in a number of projects, the patch notification which was mentioned in the present–in the initial presentation, and how to do connectivity. There's nine elements in the strategy.

So this strategy is applicable to both the OAG recommendations and to do–going ahead with NERC because it's going to require our different groups at Manitoba Hydro to work together, and so we're defining what the areas are that we're looking at and where the lines of responsibility are.

Mr. Eichler: Coming back to your lines that you were referring to in regards the areas you're trying to focus on, how are those lines established?

Mr. Reitmeier: Okay, the working groups made some recommendations and those recommendations are taken to the technical advisory committee, which I chair, and go up to the security council. So recommendations come up as to what the responsibilities are and then it goes all the way up to the security council to approve.

Mr. Eichler: So then just to take it to the next step then, what training do these people have in identifying these, and how is that established for him to be able to identify a risk or a possible risk and then get that information back to that working group you're talking about?

Mr. Reitmeier: So on that working group there were people from corporate IT and IT security, and they are used to dealing with identifying risks. But, getting back to our plan to address the office of the Auditor General's recommendations, we are implementing a new risk methodology for industrial systems and that is going to be the primary system that we're going to use to assess the assets with. So it's coming for the industrial control systems.

Mr. Eichler: I–if I can switch gears, I'd like to ask the AG a couple of questions in regards to the jurisdictions that was in your opening comments that you had based some of your analysis on. What jurisdictions would you have based those on? Would it be other provinces or is there other electrical supply companies where you are able to identify some of those risks that Manitoba Hydro may be at and what basis did you base that on? Is it on those jurisdictions or was it based on what you found?

Mr. Ricard: If I understand your question correctly, you're referring to what's–to the standards that we used when we did our site visits and what's–what we compared Manitoba Hydro to. Because we compared them to–I'm just trying to find the–we compared them to Public Safety Canada's standards that they had in place for industrial control systems, not just for utilities but industrial control systems overall. So there isn't a jurisdiction, but it's Public Safety Canada that publishes the standards.

Mr. Eichler: That organization, then, how is it comprised and how is it made up?

Floor Comment: Maybe I'll pass that question on to my colleague.

***** (15:00)

Mr. Doug Harold (Principal, Office of the Auditor General): Public Safety Canada is the federal organization responsible for industrial control systems as well as the Canadian Cyber Incident Response Centre. So they're basically Canada's leading experts with respect to cybersecurity. So they published a document in 2012 that outlines–and it's quite an extensive document outlining all the controls that they would expect to find at a minimum for any organization or business that runs industrial control systems.

Mr. Eichler: Is it based upon companies that are owned by the provinces or is it on free enterprise as well?

Floor Comment: It is–

Mr. Chairperson: Mr. Harold.

Mr. Harold: Sorry. It–the document itself is open-source and it's for anyone, but it is also directed towards governments and provinces.

Mr. Friesen: Earlier in our discussion this afternoon, I know Mr. Thomson and some others referred to the consulting firm that was contracted to do the preliminary work, and the comments from Mr. Thomson were that the engagement was successfully completed.

I wanted to ask if, within the context of that engagement, whether that consulting firm issued an opinion about the vulnerability within Manitoba Hydro compared to other companies or entities they had worked with, because I know you did mention in the remarks that this is a company that comes well recommended with experience in this area. I'm trying to establish what is the relative vulnerability of our utility as opposed to other companies.

Mr. Luce: So we're talking about Lofty Perch in terms of identifying the initial work that they've done for us through the risk assessment methodology and in the high-level implementation plan. Lofty Perch's view in terms of–and, No. 1, they did not provide their assessment as to the state of ICS at Manitoba Hydro; that's not what we asked them to do. But they did provide anecdotal comments around, you're about where the utility industry is; you're probably no better, you're probably no worse, and, as a matter of fact, we think, in some areas, you might be better.

So that's the extent of their comment or observation relative to your question.

Mr. Friesen: If I could–and I understand this chapter has already been considered at this committee, but I just wondered if I could ask for a little bit more detail as to what that engagement did actually entail. I know some information was already provided this afternoon, but just so we could understand as committee members, what was that contract specifically tasking that company to do for Manitoba Hydro?

Mr. Reitmeier: So we had two key deliverables on the Lofty Perch engagement. One was the strategy document, moving forward for the next five years, and the other one was providing us with a–what we call a risk framework.

And so, at a very high level, what the risk framework does, it integrates risk into our organization in three different tiers, three different levels. At the highest, it is called the organization level, which would consist of the–primarily at the security council level, and that–the–so the tier 1 level provides information to the second tier, which is the process level. And so–come–governance comes from the first level down to the second level. The process level is where the technical advisory committees sit, and we provide the plans and further direction to the operation level. So those are the three levels: there's the organization, process and operational.

At the operational level, that's where the work really gets done. That's where we identify the assets, we do the assessments, determine what the–which ones have to be mitigated and which ones can't be mitigated. That creates a risk registry that moves back up to the middle tier, which then goes back up to the government's level, and then we integrate the risk registry into the profile that we talked about having to go into our Corporate Risk Management Report.

So it's really a framework that takes risk and integrates it into the organization, into our business process, into our operational levels and, really, ultimately, into our corporate risk management process. So that's the essence of the framework.

Mr. Friesen: Thank you for that response. I'm also noting that in Mr. Thomson's comments, then, he referenced the fact that Lofty Perch, this same consulting company, will also be engaged to now assist in kind of a second phase of the work. And my colleague had asked earlier what was the value of the contract on the first contract with Lofty Perch. What is the value of this second contract, and then if you could just describe in a little more detail than was offered previously, what is now the nature of this next step phase 2?

Mr. Reitmeier: The next contract was for $450,000, and what's involved is the provision and customizing of the templates to do the assessment of an asset, collect that information from a site and, well, actually, complete the process in terms of what is the risk for that site. So we're having Lofty Perch go into–we haven't confirmed this yet–but up to five sites, and we're looking to do a combination of generation, transmission, old and new sites, and we think this is necessary to fast track us into being able to do more sites on our own later on. So they're going to help us develop the process, go through a number of critical sites and then we can carry on after that, and we have some targets that we have to meet in terms of NERC compliance in getting a number of critical sites done.

Mr. Chairperson: Mr. Luce, you have additional comment?

Mr. Luce: Just to top up on what Glen had said, the whole idea is to get to a–to build a repeatable process that Manitoba Hydro staff can take to these locations and apply the methodology, determine the risk and to identify mitigation plans.

So, as I said earlier, this is a bit of an emerging threat within the industry. Lofty Perch, in addition to helping us on the technical components of it relative to template development and so on and so forth, will actually be partnering with us through the first number of locations to transfer that knowledge and develop those skills internally so we can take this on ourselves.

Mr. Friesen: Will this new engagement with Lofty Perch be–is this a tendered process by which you're engaging with this company?

Mr. Luce: This would not be a tendered process. It's a continuation of the initial engagement–albeit it's different–continuation based on the understanding knowledge and what they bring to the table relative to there not being too many of these firms in the country in this area.

Mr. Friesen: Going into a slightly different direction, I was looking at page 371 of the Auditor General report and thinking back to comments that were made earlier this afternoon when we talked about that security breach that was made the one time, and I recalled the words of this report where it says that these threats to control systems are often downplayed, and so, certainly, I don't take any comfort in the idea that it's only happened once.

You know, I agree, when you say, as Manitoba Hydro, that we need to be continuously vigilant, and I want to proceed with caution here and with sensitivity, but I'm thinking right now, as we read the headlines and we know that Manitoba Hydro right now in the province of Manitoba has a very ambitious multifaceted project involving transmission, new power generation, we know that Manitoba Hydro is often in the news. There's a lot of public reaction to the plans, both positive and negative, and even at this time we even know that up north, you know, First Nation communities and some places are expressing opposition to the plan, and even now Manitoba Hydro's making strategic decisions to build in certain areas and just to allow, perhaps, a cooling-off period to take place as they contemplate next steps.

What I'm thinking about is: is Manitoba Hydro, even as all these things are taking place, are–is the company taking steps to heighten that kind of security in and around assets? Are they increasing–perhaps what I'm asking is this: In the same way that governments and other entities assess risk and then raise a level of, you know, of risk, you know, within the company, does Manitoba Hydro also increase that risk alert in regard to their capital plan going forward?

***** (15:10)

Mr. Thomson: I think what I'd offer in this area is we're obviously sensitive to potential threats throughout the system, and there is a shift in mood, if you will, across Canada as it relates to some of the issues you referred to. We have implemented additional physical security monitoring capabilities, again, at critical sites–I don't want to name any of them–but so that we're in a better position to observe. You have to appreciate that when you're–when you’ve got linear assets like we do, it's virtually impossible to station surveillance and prevention at every single asset. We're–we–but we have heightened the capability to observe, and this does dovetail with what we're doing in the whole area of corporate security, physical security, IT security, and it's a process, like I said, that's going to evolve over time.

But we do have additional capability, and that happened before we got the Auditor General's report. And it was fortuitous, or it certainly paid off, if you will, in the crisis that we had last fall around–at our Jenpeg generating station we had an awful lot more intelligence that–than we would've had a year earlier in terms of what was happening on the ground, and it facilitated our activities and our co-ordination of response with the RCMP and in other ways. And I don't really want to put anything else on the record as it relates to that.

Mr. Chairperson: Mr. Friesen, I think we're skirting kind of an envelope here. We don't want to go too far down that path, but if it retain–pertains to the report we're talking about, we can go back there.

Mr. Friesen: I do appreciate that comment and that response from Mr. Thomson.

On a different issue, I wanted to also engage the acting Auditor General this afternoon just with respect to recommendation 2, and this afternoon we heard Mr. Thomson indicate that as far as Manitoba Hydro is concerned, they consider the recommendation to be implemented. My question for the acting Auditor General would be that, then, in the opinion of the Auditor General's office, are they satisfied with the work that has been undertaken and would they concur that that goal has been met with regard to recommendation 2?

Mr. Ricard: So the–as I mentioned in my opening comments, our follow-up process on this report and on these eight recommendations will be conducted this summer; it'll be as at June 30th, 2015. Certainly, we heard from the president of Hydro talk about the progress they've been making on implementing the recommendations. I think everything I've heard to date sounds quite positive and quite clear to me that they're taking our recommendations seriously. So recommendation 2 is very specific in terms of adding it as a risk profile. I've not seen the November 2014 risk report, so until we do the follow up, I can't really comment on where we would land in terms of satisfaction with implementation.

Mr. Chairperson: Thank you, Mr. Thomson, and your managers there.

Last time we discussed cybersecurity at this committee it was to do with core government, and I do recall the Auditor General at the time and staff talking about many times intrusions are not detected because the individuals or groups are coming in, looking around, perhaps not doing anything, sometimes extracting information unbeknownst to the network that they have acquired access to, and that was definitely one of their concerns at that time for the core government. You know, you've talked about one incident that you were aware of and these others are more difficult to detect, and how would Hydro go about detecting those types of intrusions?

Mr. Thomson: I'd refer that one to Mr. Reitmeier.

Mr. Reitmeier: On our corporate security IT environment we've–just in the process of implementing what's called a security event incident management system, and in essence what it does, it correlates information from a number of our security systems to look for patterns. And that's essentially what it's there for, is to, among other things, look for anomalies such as persistent threats.

So we've put that in place, and when Bryan mentioned that we had $2.8 million that we're spending and planning to spend on our security, one of the things we're going to do is put that–SIM, it's called–that tool on–in front of all of the industrial control systems.

Hon. Jon Gerrard (River Heights): Several questions, let me start with–the Auditor General's report appears to have come at quite an important time in terms of where we are with a changing cybersecurity world and so on. So I take it that it was a helpful wake-up call in terms of the need for a major effort in this area. Would that be approximately correct?

Mr. Thomson: No, we–as I indicated at the outset, we appreciated the input and the report that we received. It did highlight some areas that had yet to be addressed. Obviously, it's going to be a significant undertaking, and we're at a point in a process right now that we have to move through, so, but it certainly was well received by me and our executive team. We certainly don't want, you know, to have risks and threats that we can't manage on behalf of the people in this province.

Mr. Gerrard: One of the issues that the Auditor General addresses is concern about what he calls–is called a gap issue, right, that initially there was a sense that if a system was isolated, that it would therefore be safe. But, I mean, as you found at Riel that there could be laptops or USB ports and so on which could certainly bring viruses into isolated stations. Can you talk a little bit about the relative importance of, you know, addressing things in gap areas where there is–they are isolated versus those things which are centrally collected?

Mr. Thomson: At a high level, I can. Certainly, the–in–and that was an explicit example that was highlighted in the report, where it's not networked, it's not connected to the Internet where you would rely on firewalls and other actions, and I think that was a vulnerability. It's–the training awareness and other protocols that will be developed around that specific type of risk so that we can manage it, those are things that have to be put in place. Is that the top priority? Again, I think it's asset specific, but it–but creating that awareness amongst people that have access to and do work on and do maintenance and do updates on those systems, those people need to be aware of and build that into their protocols as they go forward.

Mr. Gerrard: Just to understand the system, I think I remember being told a number of years ago that there was a capacity in Manitoba Hydro to alter the flow from central direction so that you could have at each dam the flow going up and down, and that could be adjusted to the power needs, and that this was one of the big advantages of the Manitoba Hydro system. But that would suggest a pretty tight connection between the operation of individual dams and the central system. Is that the way it works?

Mr. Thomson: At a high level, yes, the system control centre has the ability to bring up units and down. We also have the capability, obviously, to override that manually, and so there are fallback procedures in place in the event of a communications interruption, for instance, or to address that if–would you add anything to that?

***** (15:20)

Mr. Chairperson: Mr. Reitmeier.

Mr. Reitmeier: You can always fall back to manual operation if you lose–

Mr. Chairperson: Mr. Reitmeier, I think we're going to have to get you to speak up a little bit. Even though you're right beside Dr. Gerrard, we can't necessarily hear you down here.

Mr. Reitmeier: You can always fall back to manual operation, as Scott was indicating, when you have failure of a communication system or–you know, there's many different types of devices in industrial control systems. We think of, you know, Windows operating systems and those kinds of things, but there are many different types of devices that are called 'programmagle'–programmable logic controllers. Before, they used to be hardware relays. Now they are a little computer–just like we have in our fridges and those kinds of things, we have little computers, well, those are programmable logic controllers.

So all those are all part of the assets that we're talking about having to assess in these stations. So it's not just the, you know, what we think as typical computer systems, but it's all the devices that need to be cybersecured.

Mr. Gerrard: I think that one of the things that Manitoba would look for some level of reassurance on is that, since you've got the systems controlling flow in dams, that, you know, there's not going to be some unexpected dramatic increase in flow that you can't control because a virus got in. Maybe, you know, just in terms of, you know, addressing this issue, hopefully providing a little bit of reassurance so that, you know, Manitobans can have confidence in the system.

Mr. Thomson: Again, the Auditor General's report said that one of the areas that there was–paraphrasing, but that a significant degree of reliance was placed on our NERC compliance activities and that we needed to go beyond that, and we accept and agree with that and we're actioning that.

Having said that, the critical assets around the system control centre being able to manage the flow of power, bulk power, is one of the areas that had been addressed. So there are protocols in place for dealing with that. I think that we can take some comfort from that as it relates to that very significant item for the province.

We need to do more. Our overall corporate risk management framework, the–not just around cybersecurity but managing all of our corporate risk, does assess the likelihood of an occurrence and the magnitude of an occurrence, and the amount of action and effort that we take at addressing those things is based on the overall threat. So the items that we might address two, three, four years down the road are going to be the things that, even if they were to occur in the interim, would have less of a financial impact or operational impact on the system. We are–will be addressing the risks and the risk assessment through the framework in that fashion. So we're going to be–we've–our system control centre, our backup system control centre, which manage the overall bulk power flows, have already been–we've got a level of security around those, and that's–and we are compliant with NERC and that's–you can't rest on your laurels, and that–those standards are evolving too.

But I think that people can take some significant comfort from that. And, no, just because it hasn't happened doesn't mean that tomorrow it might not; I accept that as well. But, in all the years that we've been operating here, we haven't had a serious issue.

Mr. Gerrard: Let me ask the question in a slightly different way. There was discussion earlier on about the manual backup. Right, I mean, if there was a problem, how quickly would it be identified and how quickly could–would the people in Manitoba Hydro be able to respond with a manual override if there was commands that were given that were inappropriate?

Mr. Thomson: Again, as it relates to the bulk power system, we've got monitoring processes in place in real time around that, so if something goes down we immediately would revert either to the backup system control centre capability or then the backup to that is the manual activity.

You–I compare and contrast that with an outage on a residential street, that a transformer goes down–not that that's connected to the Internet or anything, and our–we don't have smart-grid capability yet at that level, but if something happens there, it may–it–we don't have automation in that. We do have surveillance on a lot of our transmission assets, visual surveillance for identifying physical problems, and so it's varying degrees of capability across the system.

Mr. Reitmeier: Our control centre has over 35,000 points that are inputted into it, and they're monitored every two seconds. So, if some individual function out there that's important to the bulk power system is starting to act up, our control centre will know within a reasonable amount of time.

To the example that you gave about, you know, oh, let's say water levels are not–so we really–and we put a lot of security around our control centres, more so than our corporate IT security because it is the–we call it the crown jewels, if you will, of our system. So that's really the protection we have. If something starts to act unusual out there, our control centre should know within a very reasonable amount of time.

Mr. Gerrard: Okay, no, that's very helpful in terms of having a better understanding of what risks have already been, you know, avowed for and planned in case there were problems.

One of the things that concerns me about the plan that's being developed is that you've got somewhere around 130 different sites. The plan is address five sites as priority sites. Site No. 130, it sounds like may not come up to–for eight years, but it seems to me that to some extent there's an alternative approach which might get you much faster to where you need to be.

I mean, suppose, for example, that you've got 130 sites and you train two people per site in being able to, you know, implement the optimum industrial control system at each site, then you would be able to network those 260 people and as you are making and adapting changes to a changing environment. Because, I mean, the–cyberspace is always changing in terms of the nature of the threats and the viruses and so on, that you might have a response which could be much faster than eight years if you were to approach it in this fashion as opposed to let's go start with the top five and then do the next and the next and the next. I just would be interested in your comments.

Mr. Thomson: I think as–we will adopt things as we learn, as we go along, obviously, but one of the reasons that we've engaged an industry-leading consultant on this, this is beyond my area of expertise by a long, long measure. I think that working with people that are on the front edge of developing protocols around these things and having them assist us and roll it out, there's a trade-off between the cost of implementation and the risks that were being–that we're mitigating.

So the–having not gone through the full inventory, and we may be able to accelerate that schedule and gain greater assurance as we move forward, we're certainly not open to–sorry, as I–we're certainly open to looking at alternative ways of achieving the result.

Mr. Luce: I just might want to add that another part of this that we're looking at and come up to the OAG report as well, is the physical security dimension to this as well. Inasmuch as we might have 130-odd locations that we would deem to be critical over time, we're also looking at mitigation efforts on the physical side in terms of hardening systems, hardening doors, camera surveillance, 24-hour monitoring and things like that as well.

So as much as we talk about the–call it the IT threat, we're also looking at it from a physical point of view in terms of hardening those sites as well.

***** (15:30)

Mr. Gerrard: I–what I've seen is that there is a traditional way of looking at something like this, which might be an example of what happened with Y2K, that there was an issue that had to be addressed as we moved into the year 2000. And so, once that was addressed, I mean, it was done and, you know, for another millennium we may be okay.

But, in terms of what we're dealing with here, in terms of physical and, you know, electronic and cyberspace threats, we're probably looking more in terms of an ongoing process in which we have to be able to adapt as the world changes and as software and other approaches change because we're in an era when things are pretty dynamic in this area and that when you are addressing physical and cyberspace and electronic issues, that it would seem to me that if you trained people, you know, to be able to be on top of what's happening at each site, that you decide, oh, well, we've got to check the physical structure of doors, well, you can send that message out to the person who's responsible at each site and get a quick response rather than having to do the full analysis of five sites, you know, and it–not that you don't have to go into some sites in depth just to make sure that you have a comprehensive approach, but that if you had a network of people around the system who were really highly trained, that you could be implementing improvements at all sites as you go rather than just implementing improvements at five sites and the next five and so.

Mr. Luce: And part of the–one of the recommendations relative to the OAG is training and creating awareness, and we're following up on that. And I think it's important to understand that this is an evolving process as well. As we get into it, we might change our thinking relative to, you know, to your point, is there a way–this is all about building internal capacity within Hydro to be able to do this and at what pace. And as we work our way through this, you know, as much as we talk about a list of the–in and around 130 or so, we know where we need to start for certain, and we know that the ones that are at the bottom of the list are, you know, minimal risk per se. But that doesn't mean to say we're always going to float around the top and not worry about the middle, and that'll evolve as we go through the process. I would expect that to be the case. And we've gotten guidance from, you know, the consulting firm that we're using, as well as the audit, how to tackle this beast. So.

Mr. Reitmeier: I think, once we get through the first five, we're going to have to assess how we're going to tackle the next subset, and perhaps we can look at some of the ideas that you presented, Dr. Gerrard, although I will say that there aren't a lot of people on the industrial control systems areas that support these systems, and the ones that do, security is just a very minor part of what they do. So there's certainly a skills-set requirement here, and we'll have to see how we'll be able to do that and get the training and how many people can do that. So that–there's a skills-set gap there for sure.

Mr. Gerrard: Now, I mean, I note and I thought it was very important that the Auditor General was talking about training, and although you have a skills-set gap and not very many people with that precise knowledge, you've got a lot of people who are probably, you know, 80 or 90 per cent there, that if you gave them 10 or 20 per cent training, they would be in a position, because of their knowledge of other security systems or their knowledge of their IT systems, to be able to be very effective, and I suspect that that may be part of what you need to look at.

I'd be interested in having the Auditor General sort of comment because of the, you know, the training and the suggestions that were made in the report and how you would see this rolling out.

Mr. Ricard: So the recommendation that we make on training is really dealing primarily with security awareness. But, to deal with Mr. Gerrard's comments, you know, we make a comment in the report that to do these risk assessments requires very specialized knowledge, and we did express a concern that that knowledge would not necessarily be in-house. So we, Doug and I personally, as we were listening, we were pleased to hear that you had gone outside for that expertise. But certainly a risk-based approach to the way I'm hearing it sounds logical to us, doing the five and then learning from that experience and then moving forward.

So, you know, the only comment I would make with respect to–from what I could hear and I must admit many of the comments were inaudible from here because the commotion behind me or just the–I could barely hear you, but, you know, it does require specialized knowledge that will be hard to find. It certainly would be hard to have it at each location if I understood what you were suggesting.

Mr. Gerrard: I'd like to come back to one item which came up earlier on, and that was the incident at the Riel station. And the Riel station, I believe, was to be receiving the input from Bipole III, among other areas. And perhaps you could provide to the committee a little bit of an understanding exactly where the Riel station is, at this juncture what–you know, what traffic it's handling and what the sort of immediate risks and so on would be at the Riel station site.

Mr. Thomson: We're able to transfer power between Dorsey and Riel. Riel's obviously not hooked up to Bipole III yet. We're–the switchyard's there; the site prep has been done; and we'll be in process of–we've contracted with Siemens and Mortenson to install the converter transformers both in the south and the north for Bipole III, so we're a number of years away from having power transferred on Bipole III. So it's really just–it's a local redistribution and backup today. Like we've got reinforcement in the system and the capability, and ultimately the idea is to build a ring around the city of Winnipeg so that we've got multiple points of backup for–and input into the system.

Mr. Gerrard: Now, in terms of the Riel system, it's obviously talking back and forth and interacting with Dorsey. What's the potential if the system in Riel was infected for a virus for that to get into the rest of the system?

Mr. Reitmeier: The system in Riel is a local network and it's not connected to any other network, so the potential would be very rare for it to get–it would have to be transferred manually.

Mr. Ted Marcelino (Tyndall Park): Do you plan any redundancies in the system?

Mr. Chairperson: Sorry, would you repeat the question, Mr. Marcelino.

Mr. Marcelino: Are there any redundancies that you have designed into the system?

Mr. Reitmeier: You're referring to the–which system?

Mr. Marcelino: Sorry, I mean, if you were designing something that will protect us from hacktivists, do you have any backup plans so that if there was an attack, like the blended attack that was mentioned, will we survive?

Mr. Chairperson: Mr. Reitmeier. *[interjection]*

Sorry, Mr. Reitmeier. Please continue.

***** (15:40)

Mr. Reitmeier: Many of the systems are designed with redundancy, especially if they're designated critical, and that's no guarantee, though, that you would–you could not lose both systems. It would be rare to lose like two computer systems, but most of our critical systems, like our control centres, even in corporate IT, our systems that we declare very important, we have the storage and the networks duplicated at another site. Within a station, equipment that's critical to the operation station, it will have redundant systems.

Now, you have to–security is all about risk, and you also have to allocate your resources not only to prevention but to detection and to recovery. You know, the redundant systems is part of the recovery. We're putting more and more tools on detection. This SIM tool that I mentioned earlier is all about detection, and I think we're learning over the last half dozen years that we need to allocate more resources to detection and recovery. There's no guarantee. You can spend every dollar Manitoba Hydro has on physical and cyber security; there's no guarantee that there won't be a problem. It's all about managing the risk.

I don't know if I–think I've answered your question.

Mr. Marcelino: Regarding employees, because even if you have all the systems in the world, it's still managed by employees and the threats could be from retiring employees. Have you taken a look at that too?

Mr. Reitmeier: So employees that are working on critical systems, specifically our NERC systems, have to go through a special security check, and there's also, within a specified time period on those systems they have to be removed from access to–like, if they're terminated or they leave the organization, they have to be terminated within seven days. Our new compliance standard is moving. They need to be removed from all systems including physical, cyber, and that's heading to 24 hours. And so today we're at seven days. They have to be removed from physical and cyber systems.

Mr. Marcelino: That's interesting. Thank you.

Mr. Reitmeier: Well, yes, it leads to some co-ordination activities when you think about how many systems an employee has access to.

Mr. Marcelino: That's it. Thank you.

Mr. Chairperson: Any other questions for this afternoon?

Seeing none, does the committee agree that we have completed consideration of Chapter 8, Managing Cyber Security Risk Related to Industrial Control Systems of the Auditor General's Report, Annual Report to the Legislature, dated March 2014? *[Agreed]*

Thank you. I would like to say thank you to the Auditor General–acting Auditor General–and staff, Minister Robinson, Mr. Thomson and your staff for a good afternoon and to our Clerks, researcher, Hansard staff and, of course, to our page. Thank you, everyone.

This concludes the business before us.

The hour being 3:45, what is the will of committee?

Some Honourable Members: Rise.

Mr. Chairperson: Committee rise.

Before we rise, it would be appreciated if members would leave behind any unused copies of the report, so it may be collected and reused at the next m eeting.

Committee rise.

COMMITTEE ROSE AT: *3:45 p.m*

The Legislative Assembly of Manitoba Debates and Proceedings
are also available on the Internet at the following address:

http://www.gov.mb.ca/legislature/hansard/hansard.html