Chapter 3
Data Centre Power Interruption

Contents

Data Centre Power Interruption

Main Points

Background

3.1 The New Brunswick government's wide area network and supporting network infrastructure play an essential role in delivering programs and services to the people of New Brunswick. Any interruptions in availability of this network can place severe restrictions on the delivery of critical government programs.

The 9 June 2014 loss of system access had significant adverse effects on the delivery of government programs and services

3.2 Following a power outage on 9 June 2014, a failure of one of the Province's electrical backup power systems caused a mainframe and multiple server failure in the Marysville Data Centre. This led to a major loss of system access within government for that day and caused rippling effects over the following two weeks. The loss of system access had significant adverse effects on the delivery of government programs and services.

3.3 In September through November 2014, the Auditor General of New Brunswick (AGNB) completed a review of the events and circumstances around the interruption in information technology (IT) services.

Scope of our work

3.4 Our work focused on reviewing the Marysville Data Centre and its exposure to risks related to utility power outages. The objectives of our review were:

i. to examine the details of the June 9 outage including the causes of service interruption and recovery efforts by the New Brunswick Internal Services Agency (NBISA);

ii. to examine examples of impacts to the delivery of government programs and services;

iii. to determine what risks had previously been identified and the extent of effort to mitigate those risks prior to the outage;

iv. to review the current state of IT risks, specific to the outage of June 9, and determine what improvements have been made or are planned; and

v. to determine whether the NBISA had business continuity and disaster recovery planning documented, tested and in place for the Marysville Data Centre.

Nature of the outage

3.5 The main components of the Marysville Data Centre backup power system are the Uninterruptible Power Supply (UPS), Automatic Transfer Switch (ATS), and standby power generator. In the event of a power outage, the UPS acts as an electrical storage device, providing instant temporary power. Meanwhile, the ATS changes the source of power for the building from the electrical grid to the standby power generator.

All three of the main components of the data centre backup power failed on 9 June 2014

3.6 All three of the UPS, ATS and standby power generator each suffered failures on 9 June 2014. Based on the evidence we reviewed, the failures appear to be independent of each other.

3.7 We consider the pervasive failure of the backup power system components highly unlikely to occur, given the multiple simultaneous failures. However, any single failure described above would threaten the provision of IT services to government.

Summary of Main Findings and Recommendations

3.8 We noted the impact to government services was pervasive and affected all government departments, as noted in Appendix I. Government programs and services were severely restricted during the outage and during the subsequent recovery. We did not measure the loss of productivity impact to government. However, after the outage, direct costs of just under $1 million were incurred to address various aspects of the outage. These costs include replacement of critical equipment.

Inadequate business continuity and disaster recovery planning at the corporate level

3.9 While we found some business continuity planning is in place at the department level, it is not sufficient to safeguard against disasters that may affect the delivery of critical government services. The exposure of government-wide IT infrastructure to risk is not captured in the current fragmented departmental plans.

3.10 We received some feedback from departments indicating crisis management was considered to have been effectively deployed. However, government response to the system failure was highly reactive. We found no evidence a formal disaster recovery plan, which would provide a planned approach for addressing these failures and prioritizing the restoration of government services from a corporate perspective, was in place prior to the outage.

Failure to implement complete mitigation strategy

3.11 Prior risk assessments were performed by third parties and did identify the backup power system as a vulnerability prior to the outage. However, despite a directive from government to the Department of Supply and Services (DSS) in 2009 to return with a plan for the ongoing operation of the Marysville Data Centre, we found efforts by the NBISA to mitigate risk were insufficient. Discussions with senior management at the NBISA indicated they made various attempts to return to the government, but various circumstances existed to prevent this. The DSS/NBISA did not implement recommendations for risk mitigation, such as replacing the aged UPS or adding additional backup equipment.

3.12 It is unclear where central authority lies to implement government-wide upgrades to IT systems and equipment. Prescribed authority appears to be disbursed throughout government departments, but apparently there is no consensus on the appropriate strategic direction of corporate level IT.

Additional safeguards have not been implemented by the NBISA

3.13 New equipment was installed, as part of the June 9 recovery, which will improve the reliability of backup power system at the Marysville Data Centre. This reduces the likelihood of a future outage. In addition, some server redundancy has been implemented between the primary and secondary data centre locations. However, additional safeguards have been recommended by industry experts, which have not been implemented by the NBISA, such as adding additional backup power system equipment and increasing server redundancy between the two physical locations.

Risk of system failure remains

3.14 The risk of system failure posed by a power outage in the backup power system remains. While steps have been taken since June 9 to increase system reliability, further action is needed to guard against future system failures. The continued operation of critical provincial government information systems could be at risk in the event of future power interruptions. Recommendations from our work are presented in Exhibit 3.1.

Exhibit 3.1 - Summary of Recommendations

Recommendations	Department's Response	Target Date for Implementation
Implement refresh program for critical infrastructure components		
3.71 We recommend the NBISA identify critical infrastructure components and establish replacement plans. We also recommend the NBISA develop and implement a refresh program for such equipment.	For critical infrastructure components at Marysville Data Centre, NBISA will take the following approach: 1) Work with Bell Aliant and the Department of Transportation and Infrastructure to establish an inventory of critical infrastructure components and the replacement schedule for each. 2) Work with Government Services Corporate Services unit to establish an on-going budget program for the refresh of this equipment. A 2015-16 capital plan for Marysville Data Centre will be developed for consideration by the Agency's Board of Directors by March 31, 2015. A multi-year capital plan will be developed for Q3 2015-16.	The target implementation date is 4th quarter fiscal 2014/15 with the exception of the multi-year capital plan which will follow in 3rd quarter of fiscal 2015/16.

Exhibit 3.1 - Summary of Recommendations (continued)

Recommendations	Department's Response	Target Date for Implementation
Define corporate IT strategy roles and responsibilities and improve strategic alignment		
3.72 We recommend the Office of the Chief Information Officer (OCIO) define roles and responsibilities related to development of corporate IT strategic development for all departments and take recommendations to cabinet that clarify corporate IT roles and responsibilities and ensure strategic goals of the OCIO, the NBISA and the departments are aligned.	We agree with the finding and OCIO will support the clarification of IT roles and responsibilities, and the alignment of strategic goals, within the ECO IT Consolidation project.	To be completed by the end of quarter 4, fiscal year 2016-2017.
Prepare threat risk assessments		
3.81 We recommend the NBISA prepare threat risk assessments, as part of its corporate IT continuity planning, and take recommendations to cabinet to further mitigate risk of failure of IT services.	For Marysville Data Centre NBISA will do the following: 1) Prepare a Statement of Work for an independent 3rd party security assessment for Marysville Data Centre based on the Trust Services and Principles. 2) Have the assessment conducted for the Marysville Data Centre. 3) Take the assessment recommendations to NBISA's Board of Directors to further mitigate risk of failure of IT services	Target implementation date is 3rd quarter 2015/16.

Exhibit 3.1 - Summary of Recommendations (continued)

Recommendations	Department's Response	Target Date for Implementation
Develop a strategy to meet industry standards for data centre availability		
3.82 We recommend the NBISA develop a data centre availability strategy to provide a level of service congruent with industry standards. We also recommend NBISA develop a monitoring process to ensure strategies are implemented to achieve the strategic vision.	NBISA will work with the OCIO to: 1) Align with the strategic vision resulting from the OCIO Integrated Telecom and Data Centre Strategy project 2) Use project management best practices for implementation of the strategy. May also require a formal governance process to oversee and monitor this implementation.	Target timeline is dependent on the OCIO Integrated Telecom and Data Centre Strategy implementation.
Develop enterprise business continuity and IT continuity plan		
3.92 We recommend the OCIO, in consultation with departments, develop a government-wide IT continuity plan, which considers all aspects of government programs, services and operations. This plan should be tested annually to ensure its adequacy.	OCIO will develop a proposal to request required people, process and technology to develop a government-wide IT continuity plan, which will consider all aspects of government programs, services and operations. In addition, OCIO already has established a working group to govern IT Risk and will also draft a general awareness communication to obtain business support for this initiative.	Proposal to be developed by the end of quarter 4 2014-2015. Awareness Memo to departments by the second week of February 2014-15. IT Risk working group ongoing.

Exhibit 3.1 - Summary of Recommendations (continued)

Recommendations	Department's Response	Target Date for Implementation
Prioritize critical services in government		
3.93 We recommend the OCIO, as part of IT continuity planning, obtain an assessment of services from each department to identify and prioritize critical systems, which require uninterrupted IT continuity.	Addressed as part of the proposal for finding 3.92.	Proposal to be developed by the end of the quarter 4 2014-2015.
Develop enterprise disaster recovery plan		
3.94 We recommend the NBISA, in consultation with departments, develop a disaster recovery plan, which prioritizes the restoration of government IT systems.	For Marysville Data Centre,NBISA will: 1) Work with departments to create a current inventory of GNB applications in the Marysville Data Centre. 2) Have departments identify departmental criticality ratings for all GNB applications in the Marysville Data Centre. 3) Seek departmental senior management input on the identification of GNB wide criticality of applications in Marysville Data Centre.	Target implementation date for #1-#4 is 2nd quarter 2015/16 Target for #5 is dependent on the OCIO Integrated Telecom and Data Centre Strategy implementation.

Exhibit 3.1 - Summary of Recommendations (continued)

Recommendations	Department's Response	Target Date for Implementation
	4) Create and document a process for ensuring this information is kept current and accurate. 5) Address overall disaster recovery for Marysville Data Centre in conjunction with the implementation of the OCIO Integrated Telecom and Data Centre Strategy project.	

Background

3.15 The New Brunswick government's wide area network and supporting network infrastructure play an essential role in delivering programs and services to the people of New Brunswick. Any interruptions in availability of this network can place severe restrictions on the delivery of critical government programs.

The 9 June 2014 loss of system access had significant adverse effects on the delivery of government programs and services

3.16 Following a power outage on 9 June 2014, a failure of one of the Province's electrical backup power systems caused a mainframe and multiple server failure in the Marysville Data Centre. This led to a loss of system access within government for that day and caused rippling effects over the following two weeks. The loss of system access had significant adverse effects on the delivery of government programs and services.

3.17 The Province owns the building facilities, IT infrastructure, and most assets at the data centre. The damage to network hardware was extensive and resulted in a lengthy recovery process. A number of critical systems were unavailable during the outage and essential data required restoration from backup after having been corrupted. The duration of the outage impact varied between departments, ranging from one to five days.

3.18 The New Brunswick Internal Services Agency (NBISA) was established on 1 May 2010 following the proclamation of the *New Brunswick Internal Services Agency Act*. The NBISA was created to provide shared services to government departments, including most IT operations and help desk services. Previously, the Department of Supply and Services (DSS) delivered corporate IT services to departments.

3.19 Network administration for the government of New Brunswick is provided by the NBISA and includes multiple service level agreements with third-party vendors. One such vendor manages the Marysville Data Centre, including maintenance of the backup power system. The Department of Transportation and Infrastructure (DTI) is responsible for facilities management of provincially owned buildings, which includes the Marysville Data Centre's backup power generator and automatic transfer switch.

Scope of our work

3.20 In September 2014, we completed a review of the events and circumstances around the interruption in information technology (IT) services within government.

3.21 We examined the management practices of the NBISA and its role in providing corporate IT services via the Marysville Data Centre. We focused on relevant details culminating in and following the June 9 outage. This involved interviewing government employees from the NBISA and DTI who were involved in the recovery process, as well as employees from the third-party contractor charged with managing the facilities and included a tour of the Marysville Data Centre. Additional interviews were performed with various departmental staff to determine the impact on government services. We examined chronology reports from the incident, service reports and invoices. We also examined prior maintenance records for equipment and risk assessments for the facility.

3.22 We did not carry out a detailed review of global IT governance or operations of the New Brunswick government. This chapter focuses on the singular power outage event. Given the technical nature of the content of this chapter, we have prepared a glossary of terms (Appendix III).

Our work focused on reviewing the Marysville Data Centre and its exposure to risks related to utility power outages

3.23 Our work focused on reviewing the Marysville Data Centre and its exposure to risks related to utility power outages. The objectives of our review were:

i. to examine the details of the June 9 outage including the causes of service interruption and recovery efforts by the NBISA;

ii. to examine examples of impacts to the delivery of government programs and services;

iii. to determine what risks had previously been identified and the extent of effort to mitigate those risks prior to the outage;

iv. to review the current state of IT risks, specific to the outage of June 9, and determine what improvements have been made or are planned; and

v. to determine whether the NBISA had business continuity and disaster recovery planning documented, tested and in place for the Marysville Data Centre.

Objective 1 - Details of the power outage

Our Approach

3.24 We conducted several interviews and reviewed chronology reports to gain an understanding of the causes of the service interruption. We also reviewed maintenance and inspection reports to determine the status of equipment prior to the outage. We did not conduct an in depth root cause analysis to determine the specific points of failure for each system component. We relied on the technician reports and other supporting documentation provided by the NBISA.

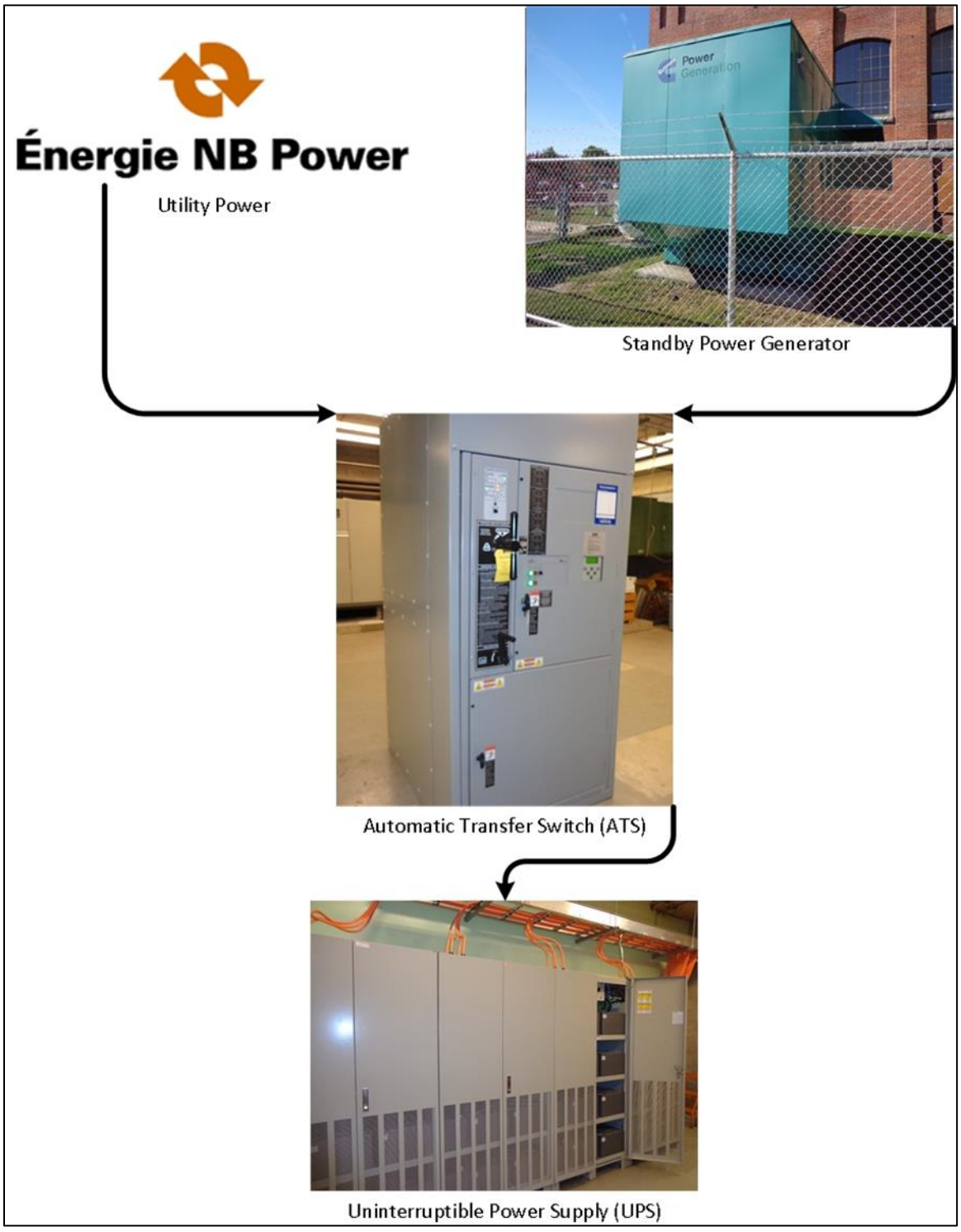
Our Findings

On 9 June 2014 the backup power system failed

3.25 On 9 June 2014, there was a power interruption in the public utility lines. At the Marysville Data Centre, a backup power system is in place to ensure continuity of service to the public when power interruptions occur. However, this backup power system failed and caused an interruption to government computing services.

3.26 The main components of the Marysville Data Centre backup power system are the Uninterruptible Power Supply (UPS), Automatic Transfer Switch (ATS), and standby power generator. In the event of a power outage, the UPS acts as an electrical storage device, providing instant temporary power. Meanwhile, the ATS transitions the source of power for the building from the electrical grid to the standby power generator. The configuration of the backup power system is shown in Exhibit 3.2.

Exhibit 3.2 - Configuration of Backup Power System



Source: Chart prepared by AGNB

Main backup components had been serviced prior to the 9 June 2014 outage

3.27 We found that, prior to the outage, the backup power system equipment was regularly inspected and maintained by contracted service technicians. The ATS had most recently been tested by a service technician on 27 May 2014 and had a mechanical failure. This issue was repaired on May 29 and two simulation tests were successfully performed. The unit was functioning normally. The generator was also inspected and tested on May 27 and was functioning normally.

Inspection report noted aging UPS component

3.28 The UPS had most recently been inspected in November 2013. The inspection report indicates the equipment status met all manufacturing specifications for operation. The inspection report had no recommended action for maintenance. The report did note that "UPS is + 22 years old and should be replaced if load continues to increase", however, we saw evidence the load had decreased over the previous year.

Backup power system worked seamlessly during 5 June 2014 power outage

3.29 We found that on 5 June 2014 during two power interruptions at the Marysville Data Centre, the backup power system worked seamlessly in both instances and no computing service interruptions had occurred.

3.30 As part of routine maintenance, the UPS battery banks were in the process of being replaced on June 9. A technician was onsite at the time of the incident. One new battery bank had been added and was fully charged, one older battery bank was in the process of being changed, and one older battery bank remained installed.

UPS power is depleted and causes a hard crash of government servers

3.31 During the utility power interruption of June 9, a mechanical failure in the ATS prevented the standby generator from supplying backup power to the data centre. As a result, the UPS reserve power was depleted and the unit shut down. Bell Aliant[1] made an effort to shut down the government's mainframe, however, the UPS failure caused a hard crash of several government servers dependent on the Marysville Data Centre.

[1] Bell Aliant is the third party service provider contracted to operate the Marysville Data Centre

UPS was found to have been irreparably damaged

3.32 A service technician manually bypassed the ATS, and brought generator power into the Marysville Data Centre. Technicians attempted to bring the UPS back online and found it to be irreparably damaged.

3.33 The UPS is a critical component in the data centre electrical infrastructure. It serves as storage of instant power during an outage, but also to condition grid power by providing protection to data centre equipment against electrical fluctuations. The UPS delivers correct and accurate voltage and electrical frequency to sensitive equipment.

Without an operable UPS, restoring grid power would leave the data centre highly vulnerable to power interruptions or electrical instability

3.34 Without an operable UPS, restoring grid power would leave the data centre highly vulnerable to power interruptions or electrical instability. Unconditioned grid power can cause performance issues and damage to sophisticated data centre equipment. Any interruption in power without a UPS will cause systems to experience a hard crash and immediately shut down despite having a backup generator. An immediate shut down of data centre systems can cause data loss or corruption.

3.35 As a result of the vulnerability posed by the damaged UPS, the decision was made by the crisis management team to operate the Marysville Data Centre facility solely on generator power. However, as Marysville Data Centre systems were brought back online, it was determined that a mechanical issue with the primary standby generator was preventing sufficient power to be supplied to the Marysville Data Centre.

The crisis management team implemented temporary measures

3.36 Temporary measures were implemented to restore full system functionality. Temporary, portable generators were rented to supplement the standby backup generator. The Marysville Data Centre was operated solely on generated power using rented equipment for 13 days.

Provincial departments and agencies experienced multiple system interruptions and corrupt data from June 9 through June 24

3.37 Subsequently, portable UPS and ATS units were rented in order to restore utility power. These components remained in place until replacement units could be installed. On August 17, replacement UPS and ATS were installed and all rental equipment was returned.

3.38 During the recovery period and following the outage, provincial departments and agencies experienced multiple unplanned and planned system interruptions through ongoing recovery efforts. Corrupt data caused issues to varying degrees from June 9 through June 24. This affected service delivery to the public, as well as the productivity of government

employees.

3.39 Additional recovery efforts were required to restore data, which was damaged or lost as a result of hard crash events experienced during the outage. A full restoration of critical government files was a gradual process lasting approximately 15 days due to the transfer speed capabilities of the storage media used and the volume of data. Exhibit 3.3 shows a timeline of events.

Exhibit 3.3 - Timeline of events

Date/time	Description
March 2009	Department of Supply and Services receives third-party report on Strategy for Provision of Computing Facilities, including the following key findings: • *Current computing facilities are highly decentralized and independently managed* • *Aliant, Corporate Information Management Services (CIMS) and each department limit the delivery of IT solutions (and benefits) to the business ("silo" mentality)* • *Business Continuity Plans (BCP) and Disaster Recovery (DR) capabilities at Department Server Rooms are poor or non-existent.* • *There is no consensus on critical applications, and therefore variable expectations for data centre capabilities and failover requirements.* • *Stakeholders not aligned on objectives for computing facility strategy.* The report also included the following key recommendations: *1. Adopt a dual data centre strategy to replace inefficient server room "sprawl"* *a) Upgrade Marysville Data Centre* • *Replace the legacy UPS with two modular UPS's to provide 100% redundancy* • *Renovate the floor to provide hot/cold aisle cooling* • *Consider updating wet sprinkler with dry charge* • *Migrate to a support model that minimizes personnel activities within the data centre* *b) Build or acquire a new data centre outside the floodplain* *c) Manage both data centres as a one logical operation* *2. Consolidate & virtualize servers and storage* *a) Consolidate department server room systems into 2 centralized data centres* *b) Apply virtualization to load balance applications on shared hardware.* *c) Use savings to fund Marysville Data Centre improvements and transformed, higher-availability facility infrastructure.*

Exhibit 3.3 - Timeline of events (continued)

Date/time	Description
July 2009	Government directed the Department of Supply and Service to implement more efficient, secure and sustainable delivery of computing facilities: • *Consolidate facilities* • *Acquire second data centre* • *Evaluate options for ongoing operation of the Marysville Data Centre at the end of third-party managed services agreement (March 2010) and return to government by December 2009 with a recommendation for ongoing operation of facility* • *Maximize opportunities for server virtualization and consolidation*
March 2010	Bell Aliant report on Marysville Data Centre Inspection and Capacity Assessment. Bell Aliant recommended upgrades to Marysville Data Centre, including replacement of UPS and addition of a second redundant UPS.
April 2010	Managed Service Agreement extended with Bell Aliant.
May 2010	The New Brunswick Internal Services Agency is established. The IT operations of Corporate Information Management Services transferred from Department of Supply and Services to the NBISA.
July 2010	Government authorizes the installation of dark fiber network infrastructure.
March 2011	March 2011 presentation from Bell Aliant highlights end-of-life data centre components, along with possible replacement costs, steps to achieve a desired end-state, value case for establishing a data centre enhancement fund.
February 2012	Government approves, in principle, the transfer of operation and management of the government's server, storage and switch infrastructure from departments to the NBISA.
April 2012	Secondary data centre is constructed.
May 2012	Mandate for the Office of the Chief Information Officer is approved by the government.
December 2013	Managed Service Agreement Infrastructure Status Report prepared by Bell Aliant is provided to the NBISA which identifies the UPS as passed end of life and assesses level of business risk associated with this component as critical.
27 May 2014	As part of testing during routine monthly inspection, the ATS experienced mechanical failure. This was discovered late in the day on May 27th, and efforts were made to have it corrected as soon as possible.
28 May 2014	The contractors dispatched staff from Ontario and Montreal to assist in the repair and a new mechanism was ordered to correct the mechanical issue with the ATS.
29 May 2014	Technicians worked on ATS and repaired the problem.
5 June 2014	Two power interruptions occurred, and in both cases, the backup power systems worked as expected. The first interruption was at 5:53 AM and lasted for 43 minutes, and the second power interruption was at 8:15 AM, lasting for an hour.
6 June 2014	Diesel tank was filled.

Exhibit 3.3 - Timeline of events (continued)

Date/time	Description
9 June 2014 – before/during power interruption	UPS service contractor in process of replacing batteries in UPS, which was recommended by the service contractor in its semi-annual preventative maintenance report when power outage occurred.
9 June 2014 – 9:17	Utility power fails. The ATS fails to switch input power source to the back-up generator. UPS continues to carry the load.
9 June 2014 – 9:30	On-site technicians proceeded to shut down the Mainframe with the UPS back-up still taking load.
9 June 2014 – 9:35	UPS battery plant is depleted and the UPS shuts down causing a hard crash of servers.
9 June 2014 – 9:44	Utility power restored and UPS failure occurs.
9 June 2014 – 10:30	After a situational assessment including an emergency meeting, the ATS is manually locked to generator power. The mainframe and servers remain offline.
9 June 2014 – 11:39	There is a brief interruption in power to the Data Centre attributed to trouble-shooting of the ATS by the technician. Power is immediately restored to the date centre.
9 June 2014 – 13:45	As the devices in the Data Centre are restored, the electrical load increases. The diesel generator is unable to provide sufficiently stable power to the Data Centre.
9 June 2014 – 14:00	The decision is executed to shut down power to the Data Centre. Mainframe and servers are shut down gracefully.
9 June 2014 – 16:00	Power restored to the Data Centre from utility power with no back-up UPS or generator. Mainframe and servers are brought back online.
9 June 2014 – 22:00	A portable diesel generator was brought onsite. The Data Centre took an emergency outage to switch to the portable diesel generator. Servers are shut down gracefully.
9 June 2014 – 23:30	Power restored to the Data Centre from the portable diesel generator. Mainframe and servers are brought back online.
15 June 2014	A planned outage is taken to perform an oil change on the portable diesel generator. The Data Centre is de-energized at 07:00 and re-energized at 14:35. During this time the facility diesel generator is repaired and tested. The Data Centre is once again powered by the portable diesel generator.
20 June 2014 – 7:20	The portable diesel generator fails due to a clogged fuel filter. This causes another hard crash to mainframe and servers in the data centre.
20 June 2014 – 8:30	Power is restored to the Data Centre from utility power with no back-up UPS or generator. Mainframe and servers are brought back online.
20 June 2014 – 22:00	Another portable diesel generator was brought onsite. The Data Centre took an emergency outage to switch to the diesel generator. The switch was completed at 23:30.
22 June 2014 – 7:00	The Data Centre is powered down for a cut-over to the temporary power stream. The temporary power stream includes all infrastructure elements of the permanent power stream but with rented/leased components (ATS, UPS, and generator).
22 June 2014 – 17:00	Utility power is restored to the Data Centre with the temporary power stream in place and operational.

Exhibit 3.3 - Timeline of events (continued)

Date/time	Description
24 Jun 2014	As a result of the June 9 crash, ongoing full restoration of data file storage containing corrupt files is completed. Files are now fully recovered.
17 August 2014 – 7:00	The Data Centre is powered down for a cut-over to the permanent power stream. New replacement ATS and UPS are installed.
17 August 2014 – 11:30	Power is restored to the Data Centre with the permanent power stream in place and operational.

Source: Exhibit prepared by AGNB
Shaded information provided by Bell Aliant. Times are approximate.

Quantitative costs

3.40 The NBISA provided a report of incremental direct costs associated with the disaster recovery effort. The report includes costs of employee overtime, repairs, rentals and purchased equipment. Exhibit 4.4 shows a breakdown of direct recovery costs associated with the outage totaling $967,000.

Exhibit 3.4 - Direct Outage related costs (000`s) as of 6 October 2014

Direct Employee Costs	$	19
Repairs		193
Incidentals: UPS, ATS and generator rentals, etc.		291
Purchase price of new UPS		200
Purchase price of new ATS		68
Purchase price of new transformer for utility entrance		64
Other: includes cost of "post mortem" analysis performed by third party		133
Total	$	967

Source: New Brunswick Internal Services Agency (unaudited). The report does not include allocations of fixed government costs related to the outage or estimations of implicit costs due to lost productivity or other affects to government.

Conclusion

3.41 All three of the UPS, ATS and standby power generator each suffered failures on 9 June 2014. Based on the evidence we reviewed, the failures appear to be independent of each other.

3.42 We consider the pervasive failure of the backup power system highly unlikely to occur, given the multiple simultaneous failures. However, any single failure described above would threaten the provision of IT services to government.

3.43 We received some feedback from departments indicating crisis management was considered to have been effectively deployed. However, government response to the system failure was highly reactive. We found no evidence a formal disaster recovery plan, which would provide a planned approach for addressing these failures and prioritizing the restoration of government services, from a corporate perspective, was in place prior to the outage.

Objective 2 - Impact on government services

Our Approach

3.44 We surveyed various provincial departments and agencies in order to provide an account of some of the impacts to delivery of government programs and services during or related to the system outage of June 9.

3.45 We did not attempt to quantify costs related to lost productivity or revenue, however, some departments provided this information in their survey responses. We included this information in Appendix II. The intent of this objective is to illustrate the scope of impact through providing examples of service interruptions. The actual duration of these interruptions varied by department. Some specific impacts of the loss of system access, as identified by departments, are described in the paragraphs that follow. A complete list of the information provided by departments is in Appendix I.

Our Findings

Department of Justice

3.46 Interruptions in system access to the Department of Justice affected the weekend remand court. Data corruption issues were noted with a number of applications. Employees were unable to access the applications required to perform their daily duties.

Department of Health

3.47 The Department of Health Client Service Delivery System was unavailable and affected the 24-hour service provided by the mobile crisis and detox unit. As well, vaccination information was inaccessible for public health immunization programs and the Department of Health Medicare application was unavailable.

Department of Finance

3.48 Department of Finance accounting systems were offline, which affected transaction and payment processing and financial reporting capabilities.

Service New Brunswick

3.49 Service New Brunswick service centres were unable to serve the public due to the unavailable systems, and online services experienced a general outage. The registries branch was unable to accept or fulfill registry applications electronically and motor vehicle online registration was down, which affected automotive dealers' ability to deliver registered vehicles.

Department of Public Safety

3.50 The Department of Public Safety lost access to systems which provide reporting on victim impact statements, case management information for probation officers, victim notification services reporting, information on admissions to

and releases from corrections facilities as well as information on those in custody. Access was also not available for the NB 911 civic addressing system, which delayed civic address assignment, however, this did not impact emergency 911 services.

Department of Social Development

3.51 The Department of Social Development safety and security alerts were not available for social workers, putting them at increased risk when performing client follow-up. Additionally, the Department of Social Development's online invoice submission was unavailable to service providers.

New Brunswick Liquor Corporation

3.52 The New Brunswick Liquor Corporation point of sale system was unavailable. Credit, debit and gift cards could not be used by customers. Additionally, warehouse management applications were unavailable.

Government-wide

3.53 Microsoft Exchange (government e-mail) went down and prevented government employees from accessing e-mails and calendars, which affected productivity of government employees who rely on these tools to schedule and perform their duties on a daily basis.

3.54 BlackBerry services were down, affecting senior government employees who rely on the devices to coordinate and perform their work.

3.55 These examples were compiled from responses received from various departments' representatives in government and represent highlights from what we found. This is not an exhaustive list of all impacts to government services.

Conclusion

3.56 The impact to government services was pervasive and affected all government departments. Government programs and services were severely restricted during the outage and during the subsequent recovery.

Objective 3 - Risk mitigation efforts

Our Approach

3.57 We conducted interviews and reviewed documentation to determine what risk analyses had been performed on the Marysville Data Centre and whether the backup power system was identified as vulnerable.

3.58 We inquired to determine what actions were planned and the status of implementation of efforts to mitigate IT continuity risks. We reviewed third-party reports and recommendations for the ongoing operation of the Marysville Data Centre, specifically with respect to the backup power system. The components of the backup power system were the focus of our work and therefore we did not investigate other recommendations by third parties.

Our Findings

In 2009, a third party was contracted by the DSS to conceptualize a data centre vision in a report called strategy for the provision of computing facilities.

3.59 In 2009, a third party was contracted by Department of Supply and Services (DSS) to conceptualize a data centre vision in a report called *Strategy for the Provision of Computing Facilities*. This report followed extensive flooding along the Saint John river in 2008. The vision was to distribute computer networking between the two locations, operated as one logical data centre. This vision would realize network server load balancing and complimentary disaster recovery across both data centres. Among the actions recommended at the time were the following items:

- update the aged infrastructure at the Marysville Data Centre, including replacement of the UPS and the addition of a secondary redundant UPS;
- upgrades to fire suppression and cooling facilities; and
- acquire a secondary data centre and implement distributed network services between the two locations.

The DSS submitted, to the government, recommendations including making improvements to the aged infrastructure at the Marysville Data Centre

3.60 On 19 June 2009, the DSS submitted, to the government, recommendations for improvements to overall delivery of computer networking services. The recommendations included making improvements to the aged infrastructure at the Marysville Data Centre and other recommendations proposed in the third-party report.

Government directed DSS to return, by December 2009, with a plan for the continued operation of the Marysville data centre

3.61 On 9 July 2009, government directed DSS to return, by December 2009, with a plan for the continued operation of the Marysville Data Centre, however, there is no evidence that this directive was carried out. Discussions with senior management at the NBISA indicated they made various attempts to return to the government, but various circumstances existed to prevent this.

A 2010 inspection and capacity assessment recommended the UPS for replacement

The UPS was identified as a single point of failure and a significant risk to IT continuity

3.62 Bell Aliant, in a 2010 data centre inspection and capacity assessment, also recommended the UPS for replacement, as well as the addition of a secondary redundant backup UPS. The UPS was identified in the inspection report as a single point of failure and a significant risk to IT continuity. Bell Aliant also recommended redundant backup power systems. In a more recent report, Bell Aliant stated: *If the UPS should fail then all government systems would lose power until the completion of the transition to diesel generator power, which is expected to occur in ten seconds or more. All affected systems would incur a "hard" power off and an immediate loss of service.*[2]

Redundancy between two data centres not yet achieved

3.63 From our work, we noted the secondary data centre was constructed in April 2012 and high transfer rate cabling was installed between the two locations. We noted additional equipment is required, however, in order to implement the proposed logical redundancy between the two locations. Prior implementation of this feature may have reduced the impact of the 9 June 2014 outage.

No replacement plans were developed for the UPS prior to the incident

3.64 We found no evidence replacement plans were developed for the UPS prior to the incident. Moreover, despite the warnings and recommendations by third parties, we found no action was taken by DSS/NBISA to replace this critical component at the Marysville Data Centre. In discussions with various stakeholders, we received conflicting reasons for the inaction. We noted that it is unclear where central authority lies to implement government-wide upgrades to IT systems and equipment.

[2] *Bell Aliant managed Service Agreement Infrastructure Status Report - 2013*

It is unclear where central authority lies to implement government-wide upgrades to IT systems and equipment

3.65 As a result of this finding, we performed a limited review of the governance structure for corporate IT services. Our expectation was that the Office of the Chief Information Officer (OCIO) has governing authority of the strategic direction of corporate IT in government. However, we found that the OCIO does not have prescribed authority to direct departments to align with overarching, corporate level, strategic goals.

Prescribed authority appears to be disbursed throughout government departments, but there is no consensus on the appropriate strategic direction of corporate level IT

3.66 We found that alignment is promoted through an executive steering committee, with representation from various departments. Prescribed authority appears to be disbursed throughout government departments, but there is no consensus on the appropriate strategic direction of corporate level IT.

3.67 The result is that significant changes to shared infrastructure, such as improvements to the Marysville Data Centre, encounter resistance due to conflicting strategies of individual departments. The NBISA, as a shared service organization, has little authority to implement significant change to the corporate level IT infrastructure. Evidence suggests that, without an explicit directive from government, significant changes to IT infrastructure may not be possible.

Conclusion

3.68 Existing risk assessments did identify the backup power system as a vulnerability prior to the outage. Although directed by government in July 2009, DSS did not return to government with a plan for ongoing operation of the Marysville Data Centre and recommendations for risk mitigation were not implemented.

3.69 Efforts to mitigate risk associated with the single point of failure or lack of redundancy in the backup power system in the Marysville Data Centre were clearly insufficient.

3.70 It is unclear where central authority lies to implement government-wide upgrades to IT systems and equipment. Prescribed authority appears to be disbursed throughout government departments, but apparently there is no consensus on the appropriate strategic direction of corporate level IT.

Recommendations

3.71 We recommend the NBISA identify critical infrastructure components and establish replacement plans. We also recommend the NBISA develop and implement a refresh program for such equipment.

3.72 We recommend the Office of the Chief Information Officer (OCIO) define roles and responsibilities related to development of corporate IT strategic development for all departments and take recommendations to cabinet that clarify corporate IT roles and responsibilities and ensure strategic goals of the OCIO, the NBISA and the departments are aligned.

Objective 4 - Review of current state of risk

Our Approach

3.73 We conducted a review of the current state of risks, specific to the June 9 outage, to identify improvements made as a result of the disaster response. Our focus was on the backup power system and strategies for IT continuity. We did not consider additional risks, which have been previously identified by third-party reports, within the scope of this review.

Our Findings

3.74 The UPS has since been replaced with a new unit, at a cost of approximately $200,000. This equipment is essential in preventing a system failure in the event of a power outage. The previous equipment, installed in 1992, was previously considered a risk due to its age.

3.75 The ATS has since been replaced with a new unit, at a cost of $68,000. The previous equipment, installed in 2003, was an uncommon model and the maintenance service provider found it difficult to find technicians to perform repairs.

The overall configuration of the backup power system remains the same, which, given our review of data centre site infrastructure tier standards, is not suitable for critical systems

3.76 The overall configuration of the backup power system remains the same, which, given our review of data centre site infrastructure tier standards, is not suitable for critical systems. Prior recommendations indicated additional redundant backup power systems and additional server redundancy would lower the threat risk posed by an outage. The continued operation of critical provincial government information systems could be at risk in the event of future outages.

The NBISA has implemented server redundancy between the primary and secondary data centres for government e-mail

3.77 The NBISA management indicated they have implemented server redundancy between the primary and secondary data centres for Microsoft Exchange (e-mail). Leveraging the infrastructure available at the newer secondary data centre, this configuration will allow e-mail services to continue in the event of down time at either location. Additional server redundancy is possible; however, this functionality is pending upgrades to equipment at the Marysville Data Centre. The redundancy made possible with these upgrades can be implemented for some critical systems. The concept for this redundancy was included in the 2009 *Strategy for Provision of Computing Facilities* report to DSS.

The NBISA is implementing improved backup process to reduce recovery times

3.78 The NBISA is in the process of implementing an improved backup media technology with a faster transfer rate. If recovery of backup data is required in the future, the new technology should reduce the time required to restore access to critical data.

Conclusion

3.79 The installation of new equipment since June 9 will improve the integrity and reliability of backup power system at the Marysville Data Centre. This reduces the likelihood of a future outage. However, industry experts contracted by the DSS have recommended additional safeguards, such as additional backup power system equipment and additional server redundancy.

Risk of IT service failure remains

3.80 The threat risk posed by a power outage due to the single point of failure or lack of redundancy in the backup power system remains. The continued operation of provincial government information systems could be at risk in the event of another power outage.

Recommendations

3.81 We recommend the NBISA prepare threat risk assessments, as part of its corporate IT continuity planning, and take recommendations to cabinet to further mitigate risk of failure of IT services.

3.82 We recommend the NBISA develop a data centre availability strategy to provide a level of service congruent with industry standards. We also recommend the NBISA develop a monitoring process to ensure strategies are implemented to achieve the strategic vision.

Objective 5 - Business continuity and disaster recovery planning

Our Approach

3.83 We held discussions with the NBISA as well as various other government organizations to determine the extent of business continuity planning in government.

Our Findings

3.84 In general, business continuity planning is a proactive planning process that ensures critical services are available without interruption. Critical services are those that must be available to ensure survival, avoid causing injury, and meet legal and other obligations of an organization. IT continuity and disaster recovery planning is captured within the business continuity plan.

3.85 IT continuity planning endeavors to ensure that operations are maintained for critical systems, which rely on IT infrastructure.

3.86 Disaster recovery planning describes how to resume business after a disruption and deals with recovering IT assets in the wake of a disaster.

Recovery of department systems and data in the event of a system outage depends on the availability of services rendered via the Marysville Data Centre

3.87 Business continuity planning for government, as it exists today, is done separately within each department. Recovery of department systems and data in the event of a system outage often depends on the availability of services rendered via the Marysville Data Centre. Continuity planning largely consists of manual processes to supplement the lack of IT services. As a result, critical government systems, which rely on IT infrastructure, remain vulnerable.

There is no documented continuity plan for IT systems should the Marysville Data Centre fail

3.88 IT continuity at the Marysville Data Centre relies on the backup power system in the event of a power outage. This does not provide for a failure of the backup power system. We found there is no documented continuity plan for IT systems should the Marysville Data Centre fail.

No documented disaster recovery plan is in place

3.89 Currently no documented disaster recovery plan is in place to prioritize the order in which critical systems should be resumed in the event of an interruption in services.

Infrastructure risks were accepted by the NBISA

3.90 Bell Aliant had identified risks related to the Marysville Data Centre's backup power system as recently as 2013 in their infrastructure status report. The list of risks was accepted by the NBISA with no documentation of a planned response related to their severity and probability of occurrence.

Conclusion

3.91 While some business continuity planning is in place today, it is not sufficient to safeguard against disasters, which may affect the delivery of critical government programs and services. The exposure of government-wide IT infrastructure to risk is not captured in the current fragmented department plans.

Recommendations

3.92 We recommend the OCIO, in consultation with departments, develop a government-wide IT continuity plan, which considers all aspects of government programs, services and operations. This plan should be tested annually to ensure its adequacy.

3.93 We recommend the OCIO, as part of IT continuity planning, obtain an assessment of services from each department to identify and prioritize critical systems, which require uninterrupted IT continuity.

3.94 We recommend the NBISA, in consultation with departments, develop a disaster recovery plan, which prioritizes the restoration of government IT systems.

Appendix I - Summary of systems impacted by the outage

We requested, from departments, a brief description of any impact/ interruption to service delivery of government programs or internal government processes as a result of the June 9 outage. The table below has been compiled using feedback provided by departments and has not been audited nor have we ensured the completeness of the responses.

Department	System/Service Affected	Type of System/Service	Impact as reported by Department
Legislative Assembly	MS Exchange Oracle Financials Application	Email service Financial	• Most services were not interrupted since department hosts own servers
Tourism, Heritage and Culture	MS Exchange Share drive Internet	Email service Data Management	• Lost productivity
Social Development	MS Exchange Internet Shared and Personal Drives NBON (New Brunswick Opportunities Network) Payroll MS SharePoint	Email services Data management Procurement Payment Intranet site	• Vendor payments were delayed • Safety and Security alerts were not available from NBFamilies, posing risk to workers and outside service providers • VEIS not available to vendors and/or would freeze or operate very slowly • Significant time and costs spent on recovery efforts • Client files could not be accessed, imposing potential risks to staff, lack of client service and backlog of data entry

Appendix I - Summary of systems impacted by the outage (continued)

Department	System/Service Affected	Type of System/Service	Impact as reported by Department
	VEIS (Vendor Electronic Invoicing System) AHESS (After hours Emergency Social Services) EIS (Executive Information System) FOS (Financial Operating System) NBClient Oracle Financials OCS (Office Communication Server) Blackberry services	Invoicing Web Portal Scheduling Internal performance reporting Departmental budgeting system Client registry Financial Communication Communication	• After hours Emergency Social Services (AHESS) staff were unable to access their On-Call Workers report used for staff scheduling purposes • Inefficiencies and loss of productivity as a result of lack of access to various applications • Significant manual backlogs accumulated in every regional and central office that need to be entered, potentially through overtime hours • Oracle outage caused several hours of re-work for internal staff and external consultants • Various invoices were found to be corrupted resulting in inefficient re-work • Calendars containing details on meetings were unavailable – individuals did not know what was in their daily schedule, nor could they access any documents for those meetings, affecting entire department's productivity.

Appendix I - Summary of systems impacted by the outage (continued)

Department	System/Service Affected	Type of System/Service	Impact as reported by Department
			• Current, historical and pending documents/reports/presentations/spreadsheets in progress or needed to take to meetings were unavailable • OCS has been failing intermittently since outage and certain outstanding issues still remain – this represents a serious degradation in efficiency • Delays and increased expenses for projects underdevelopment • Increased calls to Help Desk to report issues • Many senior staff rely on Blackberry devices on a daily basis
Human Resources	PIBA (Pensions and Insured Benefits Application) MS Exchange File SAN (Storage Area Network)	Expenditure Email service Data storage	• Staff members were severely restricted in their ability to deliver services to active members, employers, pensioners and dependents on June 9, 2014. Intermittent connectivity issues affected staff to varying degrees until Friday, June 13, 2014.

Appendix I - Summary of systems impacted by the outage (continued)

Department	System/Service Affected	Type of System/Service	Impact as reported by Department
	POLS (Pensions and Insured Benefits Application On-Line Services)	Web Portal	
	ESS (Employee Self Service) & Human Resources Corporate Website	Human resources	
	Corporate Enterprise Backup services	Data recovery service	
Justice	File SAN	Data Management	• Extensive. Many applications are deployed using ClickOnce, and the ClickOnce manifests are on the SAN. • Systems had to be restored to 5:30AM June 9, the latest reliable backup prior to the power outage • One server that housed applications could not be brought back online successfully so it had to be restored to the latest reliable backup prior to the power outage which was 7:00PM June 7
	ClickOnce	Data Management	
	JISNB (Justice Information System)	Financial	
	AEGIS (Legal Aid)	Financial	
	FSOS (Family Support Order System)	Financial	
	NOTA (Court of Queen's Bench)	Case Management	

Appendix I - Summary of systems impacted by the outage (continued)

Department	System/Service Affected	Type of System/Service	Impact as reported by Department
			• Employees had to re-enter/enter data from the period June 7th – June 13th into the appropriate applications • Outages required for repair work impacted the weekend remand court
Health	MS Exchange Internet Shared Drives MS SharePoint CSDS (Client Service Delivery System) Electronic Health Record Medicare Application High Speed Teletransmission On Line Application	Email services Data Management Intranet site Payment Claims entry	• No access to critical information • Public Health workers could not determine which vaccines had previously been administered • Mobile Crisis and Detox workers were affected

Appendix I - Summary of systems impacted by the outage (continued)

Department	System/Service Affected	Type of System/Service	Impact as reported by Department
Transportation and Infrastructure	MS Exchange Internet File server access	Email services Data Management	• Intermittent loss
Post-Secondary Education, Training and Labour	MS Exchange Internet File server access	Email services Data Management	• IT developers unable to perform duties (June 9). • Duplication of work – some work could be performed on paper while systems were down, but needed to be entered into applications once systems were back on line.
Economic Development	MS Exchange Files	Email services Data Management	• Unable to process claims and applications; reduced communication with companies. No financial loss and disruption was limited to loss of productivity.
Finance	FIS (Financial Information System) File SAN (Storage Area Network) Share drive	Financial Data Storage Data Management	• Financial information systems down
Service New Brunswick	GeoNB/Online Website		• Registries Branch unable to provide fulfillment of submissions received and registry clients were unable to present new submissions electronically.

Appendix I - Summary of systems impacted by the outage (continued)

Department	System/Service Affected	Type of System/Service	Impact as reported by Department
			• Impact on customer care at all 39 Service Centers and TeleServices. • Access to auto dealers via online application not available and access to motor vehicle registration was very intermittent. • Limited impact on specific assessment business
New Brunswick Liquor Corporation	Network Active Directory Warehouse management system VPN (Virtual Private Network) MS Exchange Blackberry	 Inventory control Remote access Email services Communications	• Point Of Sale – card tendering and gift card functionality impacted • Unable to perform basic logons, impacting all services • No remote work was possible • Store communications were hampered • Legacy Blackberry were affected – inconvenience (severity dependent on particular customer) • Lost productivity at head office and 44 stores

Appendix I - Summary of systems impacted by the outage (continued)

Department	System/Service Affected	Type of System/Service	Impact as reported by Department
Agriculture, Aquaculture and Fisheries	MS Exchange	Email services	• Unable to correspond with other users and outside clients
	Network Folders	Data Management	• Unable to access files and folders on shared drives
	DALS (Dairy Lab Systems)	Data Management	• Unable to enter quality data from prior week testing and generate reports within normal time frame – agri-food services inspectors did not receive results until later in the week. These results determine payments to producers.
	Fish Health Database	Data Management	• No specific effect identified
	Correspondence Tracking	Data Management	• No specific effect identified
Public Safety	CIS (Client Information System)	Client Information System	• Lost or corrupted data requiring long hours to restore • Client case management information was unavailable • Information used to determine a client's level of risk was not available • Manual collection of information and follow up to ensure all information is entered into CIS is duplication in work effort

Appendix I - Summary of systems impacted by the outage (continued)

Department	System/Service Affected	Type of System/Service	Impact as reported by Department
	AMANDA	Licensing and permitting system for Technical Inspection Services and Motor vehicle services licensing	• Information on clients due to be released from custody was not available requiring going through manual files • Manual calculations of sentence were required for all clients admitted to a Provincial institution
	Subsystems linked to Motor Vehicle system (Morpho and IRE/CCMTA)	Vendor's Driver's license issuance system Interprovincial Records Exchange	• Information on clients scheduled for court appearances was not available • Information on clients requiring telephone monitoring was not available; therefore some clients did not receive the required monitoring
	CDIS (Coroner Death Investigation System)	Coroner Death Investigation System	• No access to the Victim Notification information to inform victims of offenders activities as described in the program
	MS Exchange	Email services	• Licenses could not be issued
	JIS (Justice Information System)	Revenue/Expenditure	• Diminished communication
	OCS	Communications	• No access to information from Justice for probation/conditional sentence orders • Inability to host meetings online

Appendix II - Departmental costs related to the outage

We requested, from departments, a brief description of any impact/ interruption to service delivery of government programs or internal government processes as a result of the June 9 outage. The table below has been compiled using feedback provided by departments and has not been audited nor have we ensured the completeness of the responses.

Department	**Expense**	**Financial Impact**
Social Development	External – IT Consultants	Time spent on recovery efforts: - Production issues: 63.5 hours - Posting errors for NBCase journals: 0.5 hours - VPN unavailable: 25 hours - Support team hours: 91 hours - Maintenance release hours: 26.5 hours - Non-productivity of remote workers: 72 hours Total hours: 278.5 Total value of those hours: $21,500 Consultants flown in to do specific on-site work and were unable due to outage: $28,000 Support calls doubled as users continued to discover problems resulting from outage: $2,400 Total costs as result of outage to department: $51,900
	Bell Aliant Help Desk	
Department of Agriculture, Aquaculture and Fisheries	Salaries	Minimum of one (1) day lost productivity for each of approximately 284 staff members over span of the outages
Department of Human Resources	Salaries	Approximately 80 staff members were severely restricted in their ability to deliver services for the day (June 9)

Appendix III - Glossary of Terms

Term	Definition
Automatic transfer switch (ATS)	The automatic transfer switch transitions the source of power for the building from the electrical grid to the standby power generator.
Backup power system	Backup power systems use local generation at the facility site to provide power when the utility is not available. The backup power system may or may not be interconnected with the utility grid.[1]
Business continuity plan (BCP)	A business continuity plan enables critical services or products to be continually delivered to clients. Instead of focusing on resuming a business after critical operations have ceased, or recovering after a disaster, a business continuity plan endeavors to ensure that critical operations continue to be available.[4]
Backup Media	Refers to different types of data storage options used to backup systems.
Crisis management team	Formed to protect an organization against the adverse effects of crisis. Crisis management team prepares an organization for inevitable threats.[3]
Critical services/systems	Critical services or products are those that must be delivered to ensure survival, avoid causing injury, and meet legal or other obligations of an organization.[4]
Data centre	A facility housing computer systems and related components.
Disaster recovery plan	Applies to major, usually catastrophic, events that deny access to the normal facility for an extended period.[2] A Disaster recovery plan deals with recovering information technology (IT) assets after a disastrous interruption.[4]
Failover	Failover is the constant capability to automatically and seamlessly switch to a highly reliable backup. This can be operated in a redundant manner or in a standby operational mode upon the failure of a primary server, application, system or other primary system component. The main purpose of failover is to eliminate, or at least reduce, the impact on users when a system failure occurs.[6]
Hard crash	When a program stops running completely and unexpectedly, often due to external events.[8]
Standby power generator	Machine that converts mechanical energy to electricity for transmission and distribution
Grid	A network of electrical wires and equipment that supplies electricity to a large area.[5]

Appendix III - Glossary of Terms (continued)

Term	Definition
IT continuity plan	Addresses the IT exposures and solutions based on the priorities and framework of the business continuity plan.[2]
Redundancy	Refers to duplicate devices that are used for backup purposes. The goal of redundancy is to prevent or recover from the failure of a specific component or system.[7]
Single point of failure	A single point of failure (SPOF) is a critical system component with the ability to cease system operations during failover. SPOFs are undesirable to systems requiring reliability and availability, such as software applications, networks or supply chains.[6]
Threat risk assessment	Refers to the process of defining and analyzing the dangers to government organizations posed by potential natural or human-caused adverse events. An assessment of overall risk is a function of severity and likelihood of occurrence and indicates whether a mitigation response is warranted.
Uninterruptable Power Supply (UPS)	A type of power supply that uses battery backup to maintain power during unexpected power outages. In mission critical data centers, UPS systems are used for just a few minutes until electrical generators take over. The online UPS is continuously providing clean power from the battery, and the computer equipment is never receiving power directly from the AC outlet.[7]
Utility	A service (such as a supply of electricity or water) that is provided to the public.[6]

Appendix III - Glossary of Terms (continued)

Sources:

[1] National Electrical Manufacturers Association. (2014). Backup *power systems.* Retrieved October 24, 2014, from http://www.nema.org/Storm-Disaster-Recovery/Backup-Generation/Pages/Backup-Power-Systems.aspx

[2] Office of the Auditor General of British Columbia. (2010). *IT continuity planning in government.* Retrieved September 2014, from www.bcauditor.com

[3] Management Study Guide. (2014). *Crisis management.* Retrieved October 24, 2014, from http://www.managementstudyguide.com/crisis-management-team.htm

[4] Government of Canada. (2014). *A guide to business continuity planning.* Retrieved September 22, 2014, from http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/bsnss-cntnt-plnnng/index-eng.aspx

[5] Janalta Interactive Inc. (2010-2014). *Techopedia*. Retrieved October 24, 2014, from http://www.techopedia.com/

[6] Merriam-Webster, Incorporated. (2014). *M-w.com*. Retrieved October 24, 2014, from http://www.merriam-webster.com/dictionary

[7] TechTerms.com. (2014). Retrieved October 24, 2014, from http://www.techterms.com/definition

[8] Dictionary.com, LLC (2014) Retrieved December 10, 2014, from http://dictionary.reference.com/