Kawartha Lakes

Committee of the Whole Report

Report Number:	**CORP2022-002**
Meeting Date:	February 8, 2022
Title:	**CORP2022-002 Assuring Business Continuity for Network Operations**
Description:	A report to provide information about the systems outage that occurred on September 20, 2021,and outline improvements that have and/or will be implemented in order to avoid/mitigate risks associated with future outages.
Author and Title:	Kari Kleven, Manager of Information Technology Jörg Petersen, Manager of Buildings and Property

Recommendation(s):

That Report CORP2022-002, **Assuring Business Continuity for Network Operations**, be received.

Department Head: ____

Financial/Legal/HR/Other:____________________________________

Chief Administrative Officer:__________________________________

Background:

On September 20, 2021 the City experienced a catastrophic failure of its Information Technology (IT) infrastructure. This failure was the result of water infiltration from the roof of City Hall into the Network Operations Centre (NOC). This water infiltration occurred during maintenance to rooftop mechanical equipment when a seal in the assembly of the roof top unit failed, and allowed water to pass into the building. The water then migrated into the NOC. The amount of water that entered the space is estimated to have been quite small, however upon coming into contact with equipment contained within the NOC it resulted in damage to and failure of said equipment. The failure of this equipment caused a widespread disruption to Information Technology services and resulted in some loss of business data.

The equipment failure within the NOC had a broad impact on a large number of the City's information systems and applications. Recovery of these systems required IT staff to rebuild and restore servers and data. Full recovery of all impacted systems and data took 12 calendar days. During that time recovery of systems happened steadily with recovery efforts determined by the priority of the systems as identified in the IT Disaster Recovery Plan.

Rationale:

The September 2021 IT infrastructure failure demonstrated the need for direct action to be taken on improvements. Some improvements have been completed while others are still in progress. It has also highlighted the need for a review of the City's NOC to identify risks, devise an action plan to eliminate / mitigate those risks, support staff actions to manage the risks, and provide senior management and Council with a comprehensive risk management (assurance) report.

A risk assessment will identify gaps, determine the likelihood and potential impact of risks associated with those gaps, and make recommendations to close them. Our initial risk assessment has considered the five risks categories and related actions: facility; equipment; system resources; software; and operations.

Facility

Facility risk includes the location, design and systems that make up the facility where the NOC is currently placed.

The NOC is located at City Hall. It is the City's only data centre. Alternatives to reduce our dependence on a single NOC include a secondary NOC, co-location of equipment in locations owned by other organizations, and cloud services.

In 2019 a capital budget to construct a secondary NOC was submitted and subsequently funded in 2019 and 2020 in the amount of $300,000. The secondary NOC was to be located and constructed as part of the build of 68 Lindsay Street North. In order to not delay occupancy, the secondary NOC construction was deferred until occupancy occurred. The project was put on hold in 2020 due to the pandemic. When resumed in 2021, fee proposals obtained by the Buildings and Property Division estimated a total construction value of $875,000, or $575,000 more than the approved budget.

Given the significant cost increase, staff are now evaluating the possibility of hosting the secondary NOC at other City facilities or with a neigbouring municipality. Additionally, staff are developing a cloud strategy to determine the suitability for utilizing cloud services to address this need.

The City's NOC currently has many securities in place to protect the infrastructure including, but not limited to: stand by power generator; specialized fire suppression; internal flooding alarm sensors; and temperature controls and alarms.

Since the September event, the internal plumbing that posed the risk to the NOC has been rerouted to prevent further occurences. The roof penetrations are being removed as part of the City Hall HVAC project, and the sprinkler system piping is planned for relocation. Staff are further considering the potential of additional protection that would shed water, or other debris, away from the IT equipment.

Equipment

Equipment may fail for various reasons. One of the key strategies to mitigate down time in the even to failure is to build redundancy into our network operations. Where redundancy exists, as one piece of equipment fails, the redundant equipment can be utlitized which greatly minimizes or eliminates down time.

The City currently has redundancy built into our critical infrastructure such as phone system, email and Citrix servers. The City backs up data on a daily basis to mitigate lost data. Currently however, the City only has one tape drive that is able to restore data from the back up. Staff are in the process of securing a second, or redundant tape drive.

For further consideration, staff are reviewing the requirement to implement additional redundant equipment to further mitigate downtime.

System Resources

System resources risk includes items that might affect data connectivity and access to data and services through the network such as electrical or broadband services.

Staff are exploring the possibility and need to implement a redundant internet connection and phone system connectivity.

Software

Software failures can result from a myriad of reasons including misconfiguration, software bugs, data corruption, and malicious code. Since the September event, staff have replaced the back up and recovery system software which will reduce the time to recover from backup storage.

Additionally, staff are reviewing vendor support contracts to and ensure our environment aligns with vendor support requirements, and address any gaps.

Operations

Operational failures can be caused by many different events. The list of risks associated with operations failures includes, but is not limited to: the quality of equipment maintenance, system documentation, human error and potential security issues. Dealing with operational failures requires a range of mitigations and active management that needs to be constantly maintained.

Two of the key measures are a Disaster Recovery Plan which to ensure a quick recovery from any outage, and a Business Conintuity Plan provides appropriate workarounds when systems are not available. The City had both of these plans in place prior to the September event however, staff are now reviewing and updating the plans based on the recent experience.

Additionally, staff are reviewing the current structure of the IT division to ensure that there are appropriate resources and cross training to enhance the preparedness should there be a future event.

Staff will continue to monitor and identify significant risks, and devise an action plan to eliminate or mitigate those risks. The information above is intended to provide Council with the higher level view of the event and the actions taken or in progress based on lessons learned.

Other Alternatives Considered:

No other alternatives considered.

Alignment to Strategic Priorities

This reports aligns with the following strategic priorities:

- Asset Management within the goal of Good Government by ensuring municipal assets are well maintained and well managed
- Increase Efficiency and Effectiveness of Service Delivery within the goal of Good Government by promoting continuous improvement in all service areas and striving to maintain current levels of service when faced with adverse events.

Financial/Operation Impacts:

Staff are continuing to explore opportunities for a secondary site, either at another city facility or a neighbouring municipality. As those explorations conclude staff will report back to Council, as necessary, for information or direction.

Consultations:

Director, Corporate Services
Director, Community Services
Supervisor of Network Services and Client Support
Supervisor, Capital Projects Delivery, Building and Property
Supervisor, Facility Management Operations, Building and Property
Supervisor, Applications

Attachments:

n/a

Department Head email: jstover@kawarthalakes.ca

Department Head: Jennifer Stover