Committee Report

To:	Warden McQueen and Members of Grey County Council
Committee Date:	December 12th, 2019
Subject / Report No:	ITR-CW-01-20
Title:	Disaster Recovery Planning
Prepared by:	Jody MacEachern, Senior Manager of Information Technology; Evan Davis, Technology and Infrastructure Manager
Reviewed by:	Kevin Weppler, Director of Corporate Services Mike Alguire, Purchasing Manager
Lower Tier(s) Affected:	
Status:	Recommendation adopted by Committee as presented per Resolution CW03-20; Endorsee by County Council January 9, 2020 per Resolution CC13-20;

Recommendation

1. **That report ITR-CW-01-20 regarding disaster recovery technology be received for information.**

Executive Summary

Grey County staff included disaster recovery (DR) as a project in the 2019-2028 10-year capital forecast. In 2018, Perry Group Consulting assessed the business and technology requirements for DR and recommended against Grey County building and maintaining a second data center.

This report provides background on the County's DR efforts to date and outlines the technological solution County staff intend to implement to continue providing services in the event of a disaster that affects IT services. Potential scenarios in which this technology would be used include damage to the County Administration Building, primary data center, or ransomware.

The planned DR solution would cost $119,000 in the first year, and approximately $45,000 annually thereafter. Earlier capital forecasts included an estimate of $150,000 for DR services over five years. This estimate was based on a smaller amount of IT services running in the cloud. IT staff will re-assess other projects in the ten-year capital forecast to avoid budget increases in 2020.

Background and Discussion

Introduction

Grey County, like any modern business or government agency, relies strongly on stable, reliable information technology to manage its operations. Every line of work and every staff member relies on technology and technological processes in their day to day jobs, be it payroll, email, telephony, data management, patient health monitoring, legislative compliance, etc.

Grey County IT staff have implemented a range of technologies that provide some stability and resilience to the infrastructure and applications that underpin these services. Measures include high-availability in core server infrastructure (the system can withstand partial component failure); nightly data backups stored offsite, and redundancy in core infrastructure components (eg firewalls and internet connections) protecting critical services. Further, IT has in place a range of cybersecurity solutions to reduce risk for cyber threats and malicious activity on the County's network.

If, however, a disaster did occur at the County's main data center that impacted hardware, IT would be left re-pairing systems or rebuilding from scratch, with little interim technological services available for normal business services. Re-building the County's main data center could take easily between four and eight weeks.

Given the importance of the County's data and the services it delivers, it is critical that the County prepare for emergencies that impact technology. Grey County Council previously endorsed disaster recovery planning in IT capital budgets and County staff are now ready to begin implementing those projects.

Disaster Recovery Assessment

In 2018, Grey County engaged Perry Group consulting to advise on Disaster Recovery requirements and planning. The main objectives of this engagement were to:

a) identify which services were critical to the corporation, and would need to be available during a disaster, and

b) advise on technological direction for providing DR capability from an IT perspective.

Perry Group conducted business impact assessments (BIA) with each department in which departmental managers identified the services they deliver to the County or County residents. Because the BIAs were driven by business area, not technology, managers were easily able to quantify the impacts of an interruption in these services (financial, health and safety, legislative, and reputational), and in turn assign criticality ratings to those services.

Perry Group, working with Grey County IT staff, were able to identify the infrastructure, services, and applications that drive these business services. This allowed specific requirements for disaster recovery services in terms of network resources required to both store these services and run them from an alternative location at time of disaster.

Disaster Recovery Services

Perry Group used an approximation of the County's system requirements to assess whether IT should build and manage a second data center on one of their properties, or seek Disaster Recovery as a Service (DRaaS), in which a vendor would take a continual transfer of the County's data for backup and run critical applications from their network should the County have a disaster.

In terms of simple operation (storage of data at rest), Perry Group concluded it was far more efficient to seek out DRaaS services than it was to commit the resources (renovation, hardware purchases, staff time for design, build and maintenance) to building and managing a second data center.

Grey County IT staff continued to research two main options for DR:

1) Full DRaaS in which a vendor would completely manage the hosting environment and applications required to run those services at time of disaster, and

2) replicating to a cloud-hosted environment managed by Grey County.

In all cases, using DRaaS providers is estimated to be more expensive than having Grey County staff manage data replication to cloud hosted infrastructure. Cost estimates ranged from $60,000-$145,000 per year, plus further costs for initial set up and software licensing.

By comparison, using cloud-hosted infrastructure and replication software, staff estimate costs of:

Setup Costs	
Professional Services	$15,000
Virtual Firewall	$5,000
Software	$99,000
Set Up Total	**$119,000**

Annual operation costs	
Microsoft Cloud-hosted infrasturcture	$20,000
Replication Software	$20,000
Virtual Firewall	$5,000
Annual Operation Total	**$45,000**

Legal and Legislated Requirements

None

Financial and Resource Implications

Grey County IT staff have previously included $150,000 over 5 years for disaster recovery hardware in capital forecasts and budgets. This number was a best guest based on discussions with DRaaS providers and assessments done by Perry Group using only a subset of our operational requirements.

Having researched various options to provide DR, Grey County staff concluded that the best option in terms of business requirements and financial impact will cost approximately $119,000 in the first year (software purchasing, cloud hosting environment) and approximately $45,000 annually thereafter in software license maintenance and operational costs for the cloud hosted environment.

This change to the project costs will be reflected in the IS operational budget starting in 2021. Staff suggest postponing another capital project, Virtual Desktop Infrastructure to ensure capital reserves cover the DR Project through the 2020 budget year. The Virtual Desktop Infrastructure project will be reassessed in 2020 to gain a full understanding of the benefits of the project, and the full financial implications, before carrying this project forward on subsequent budget years.

Relevant Consultation

_X_ Internal IT and Finance staff

__ External (list)

Appendices and Attachments