Business Resiliency: The Hidden Threat to Your Municipality

Connell Price
ElectriCities of NC, Inc.
As technology continues to change, its rate of adoption increases exponentially. As municipalities strive to integrate technology, it becomes increasingly important for these technology “systems” to remain viable...even through catastrophic events.
If a disaster strikes, can your technology continue to provide the critical services necessary to support the residential and business needs of your municipality?
In this session, we will cover the basic business drivers for having and maintaining a Business Resilency Plan (BRP).

We will examine the following topics:
I. Understanding and Addressing Business Vulnerabilities Created by Technology

II. Planning, the Key to a Successful BRP

III. What is Your Recovery Strategy?

IV. Putting It Together: The Connections Conference IT Track Overview

Business Resiliency: The Hidden Threat to Your Municipality
The BRP is the framework to address the business requirements necessary to support technical solutions designed for continuity of operations.
I. Understanding and Addressing Business Vulnerabilities Created by Technology
Myth: “We can always go back to manual processing…”

As information becomes more instantaneous with delivery across multiple internet enabled devices, customer demand outpaces our ability to keep up when reduced to manual processing.
The Danger of the “Domino Effect…”

As systems become more complex and are spread across geographies, the effect of a single outage could have a domino effect to municipal operations including customer facing areas.
Changing Server/Computing technology has eliminated the old “rip and replace” philosophy…
II. Planning: The Key to Successfully Mitigating the Vulnerabilities Created By Technology
Start With a Documented Plan…

A preparation document that describes what you would do to continue and recover your Technology Operations after a disaster.
A “disaster” is defined as: Any major event that causes inaccessibility or inoperability to your facilities, technology & business operations…
Why Should Municipalities Plan?

Requirements:
- Concern for Constituents
- Concern for Employees
- Auditing
- Insurance (having a plan will make you more desirable to the underwriting community and will reduce your contingent insurance premiums)
- Business Partners
- Service Level Agreements
- Governance Requirements

Loss of:
- Reputation
- Business Opportunities
- Efficiencies and Cost Savings
- Public Confidence
The Most Common Type of BR Plan...

Hey Bob,
What’s our BR Plan?

An up to date resume...!
Know Your Critical Processes:

Business Impact Analysis (BIA):
Evaluate all critical operations and determine the technical resources needed to run them.

*Recovery Time Objective:* Period of time within which systems, applications, or functions must be recovered after an outage.

*Recovery Point Objective:* Point in time to which systems and data must be recovered after an outage.
Define Your RTO’s and RPO’s…

Recovery point objective (RPO):
How recent is the point in time for your recovery?

Recovery time objective (RTO):
How fast can you restart a failed application?

(RPO+RTO = Acceptable Business Risk)
Recovery Point

Objectives

PRIMARY DECISION DRIVERS

Business Considerations
- Cost
- Functionality, Availability
- Recovery Time Objectives
- Recovery Point Objectives

Technical Considerations
- Consistency and Recovery
- Capacity
- Bandwidth
- Performance

II. Planning: The Key to Successful DR…
III. What Is Your Recovery Strategy…?
Business Recovery Planning Stages...

**Major Steps**
- **Initiation**
  - Obtain Management Support
  - Identify the Planning Team and initial planning information
  - Develop Project Plan
  - Conduct Project Kickoff Meeting

- **Identification**
  - Identify likely risks/threats to cause a disaster
  - Identify business impacts of a disaster
  - Identify Supply Chain (Vendor & Partner) Dependencies
  - Identify Recovery Resource Data

- **Create Strategy**
  - Analyze and choose recovery strategies to achieve RTOs
  - Determine and document the recovery tasks
  - Analyze the organizational structure to implement the Recovery Team Scheme (i.e., who does what and how)

- **Plan Development**
  - Assemble the information gathered and decisions that have been made
  - Document the Plan
  - Publish the Plan

- **Training & Exercise**
  - Educate plan owners on its use & what to do in disaster and recovery situations
  - Conduct an Awareness Exercise and issue a Report
  - Develop tools for subsequent exercises

- **Maintenance**
  - Identify organizational changes that will require plan updates
  - Establish a maintenance program

**Actions**

**DELIVERABLES**

1. Project Initiation Charter
2. Project Kickoff Meeting
3. Project Plan

1. Risk/threat and business impact Info
2. Supply Chain dependencies
3. Resource Data

1. Recommended recovery strategies
2. Recovery Tasks
3. Recovery Team Scheme

1. Plan Template
2. Documented Plan Manual

1. Trained Plan Participants
2. Performed Exercise
3. Documented Exercise Rept

1. Maintenance Program
2. Plan Disclosure - Certifications Statements
IV. Putting It Together: The Connections Conference IT Track Overview
Three Critical Questions to Ask Your IT Department...

Business Resiliency Plan

- Cloud Computing
- Cyber Security Best Practices
- Virtual End User Computing
- Strategies for IT Financing

The BRP is the framework to address the business requirements necessary to support technical solutions designed for continuity of operations.
The evolution of cyber security has grown from a point solution to total integration into an organization’s business resiliency plan.

Learn how adopting a CDC (Centers for Disease Control and Prevention) strategy can help enhance your cyber security initiatives.

This session will explore four common sense strategies to support cyber readiness activities.
Three Critical Questions to Ask Your IT Department…

- More secure citizen & government data
- Better insights drive new citizen services and economic growth
- Reduced costs and greater efficiency
- Fully engage constituents and employees with accessible content
- Resiliency and response enablement in disasters
Virtual End User Computing (commonly referred to as Virtual Desktop or “VDI”) will be demonstrated and defined.

Municipalities, like commercial business, are faced with the challenges of delivering applications and data to people securely and reliably.

The “Commercialization of IT” and the demands of mobility drive up cost and increase risk. How VDI can help:

a) Drive down overall IT costs and increase productivity
b) Enable people to work from anywhere on any device while reducing security risk
c) Demonstrate how Disaster Recovery & Business Continuity are native to virtual computing.
Best practices will be discussed for paying for IT Assets, including software, over time.

Starting with basic strategies around leases and loans, to more usage based models where we discuss benefits and pitfalls with each tool.

We also discuss the changes in the way IT is being sold by different manufactures and providers including more subscription based approaches that may enable more flexible ways to take advantage of newer technologies at a lower overall cost.
In Summary…

- Well defined, documented and tested plans are a must for any municipality.
- Plan design is centered around the core business processes within the municipality.
- The core business process drives your RTO and RPO strategy.
- The Business Resiliency Plan provides the technical strategy to support the defined core business processes.
- A plan that is not tested, is no plan at all.

“If you fail to plan, you are planning to fail!” — Benjamin Franklin
Business Resilience: The Hidden Threat to Your Municipality
FOLLOW US ON SOCIAL MEDIA:

@ncpublicpower
facebook.com/Electricities
@ElectriCitiesNC