Every Company Needs to Prepare a Business Continuity Plan

DIGITAL SOLUTIONS CONFERENCE

CYBERSECURITY

There's been a breach!

What do we do?

DIGITAL SOLUTIONS CONFERENCE CYBERSECURITY

POWERED BY NMFTA
National Motor Freight Traffic Association, Inc.

My Business Continuity Background

- Homegrocer.com and Webvan
  - First introduction to BCP and DR

- Washington Mutual (Wamu)
  - Business Continuity
  - Disaster Recovery
  - Vendor Risk Assessment
  - Emergency Management
  - Cyber Resilience

- Continuity Source Co-founder
  - Business Continuity SaaS

- Johanson Transportation Service (JTS)
  - Created a comprehensive Cyber Resilience, BCP/DR program
  - Continuous Improvement through Planning and Testing

Why do I Need a Business Continuity Plan?

- "Business continuity provides a framework for building organizational resilience and the capability for an effective response." –DRI International, 2018, *DRI Professional Practices*
- Cyber Breach Legal Notification Requirements: Customer, Vendor, Data Privacy
- Cyber Insurance Requirements
- Cyber Resilience
  - Respond and Mitigate quickly
    - Everything we do daily to prevent attacks could be for nothing if we can't respond in a timely manner
- Business Survival

Who has the Time and Where do I Start?

- Get Support from Upper Management

- Schedule the Time in Small Chunks

- Understand Your Risks
  - Look around at your environment
  - Schedule regular Pen Tests
  - What has affected you or others in your industry in the past?
  - Talk to your department heads

- Identify Business Processes and Prioritize

- Set your Recovery Time Objectives (RTOs) based on Priority

What do Those Processes Depend on?

- Technology
  - Most People have Backups but may not have Progressed
    - Immutable, multi-media, multi-location
  - Data Center Continuity
    - Failover to another region while you recover failed region
  - Identify Applications, Data, Essential Equipment
  - Set Recovery Time Objectives (RTOs) and Recovery Point Objectives(RPOs) Based on when the Process is Needed
  - Key Technology Vendors
    - Look upstream and downstream
    - What happens if your rates provider or the cloud they use to host their service goes down?

Other Process Dependencies

- Physical Locations
  - Earthquake, Fire, Water Damage, Technology Outage
  - Easier in the Digital Age
    - Covid forced us to figure this out
  - What about Long Term Loss of Location?
- People
  - Sudden Loss of Personnel
  - Long Term Loss of Key Personnel
  - Succession Plan
- Vendor
  - Are your Vendors Prepared?
  - What's their Plan?

Incident Response

- The Time it Takes for you to Respond can Greatly affect the Severity and Outcome of a Cyber Incident or other Disaster
- Define Clear Roles, Hierarchy, and Succession
  - Everyone should know who's in charge and what role they have
- Emergency Operations Center
- Communication Plan
  - Who gets contacted and in what order
  - Who is doing the communicating
  - Include internal and external parties
  - What media and channels to use?
    - Voice, Text, Hamm Radio, Satellite phone, What's App?

Notification Channels
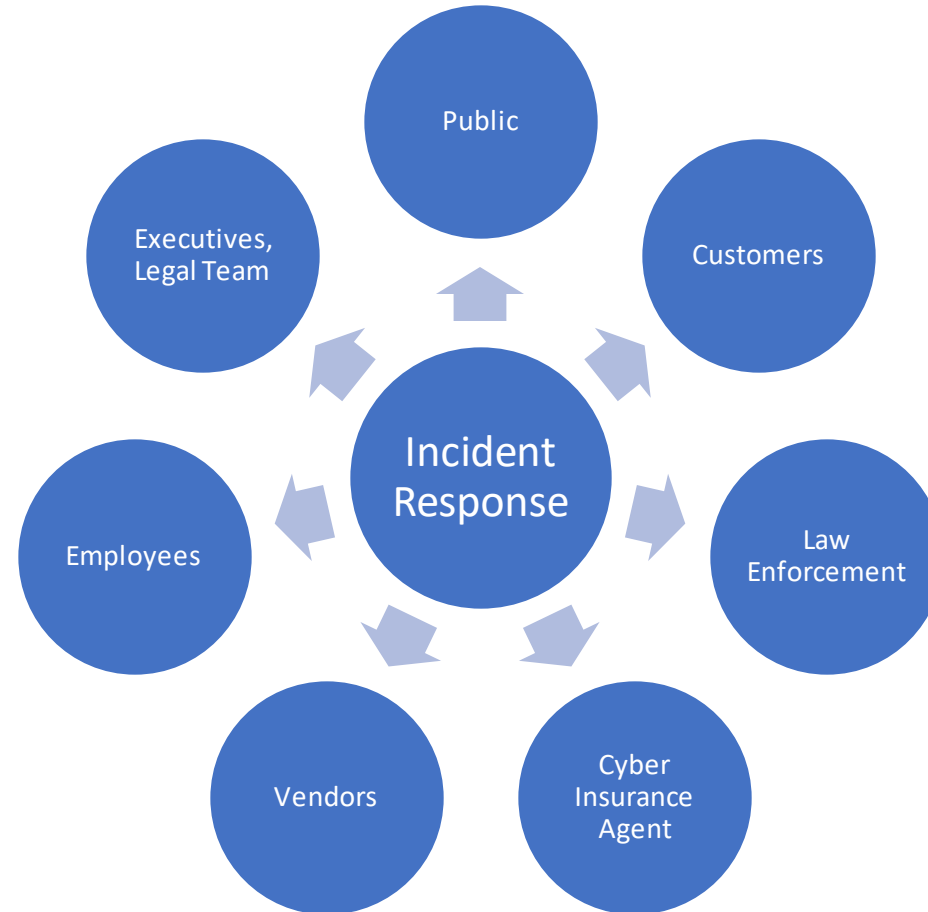
Create Your Business Continuity Plan

- Put the Pieces Together and Document it
  - Include both Recovery (Restoring) and Continuity (Running while you restore)
- Don't Assume any Particular Person will be Following it
  - Include enough detail that anyone on the team can pick it up and run with it
- Large Type, Easy to Read, Quick Access to each Section
- Include Manual Workarounds and Templates
- Update the Plan as your Environment Changes
  - Make it a part of your everyday process

Educate, Test, Update Plan, Repeat

- Business Continuity is a Work in Progress.
  - It may take several tests to get it right
  - Finding issues with your plan is a good thing
  - Involve Everyone
- Larger Drills Coordinated with Local Government
- Smaller Tabletop Exercises Based on Scenarios
- Use Real Events to make your Plan Stronger
- Apply the same Cyber Resilience Policies
  - Encrypted, Immutable, MFA, Zero Trust
  - Look for higher levels of security if using new vendors

Resources:

- https://drii.org/resources/professionalpractices/EN
- https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
- https://niccs.cisa.gov/education-training/catalog/cybrary/business-continuity-disaster-recovery-planning

Questions?

DIGITAL
SOLUTIONS
CONFERENCE
CYBERSECURITY