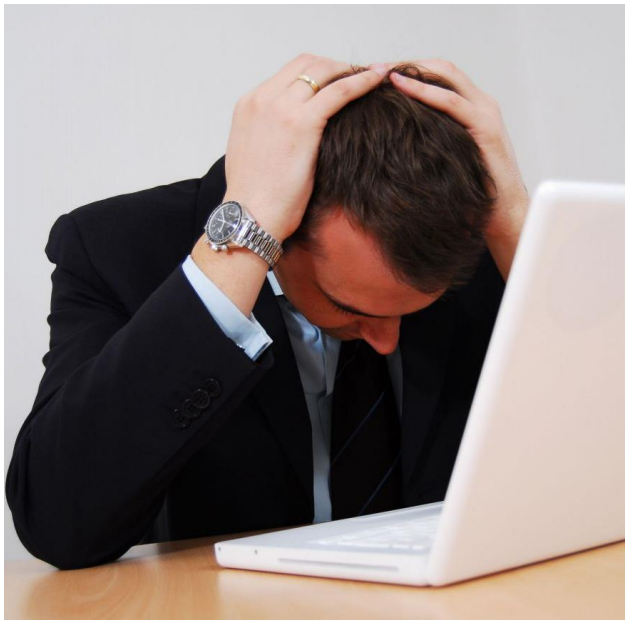
2017 Region II AAMVA Conference
CHATTANOOGA, TN • JUNE 19-22

Business Continuity Planning – Keeping Pace with New Technology

Safe Drivers · Safe Vehicles · Secure Identities · Saving Lives

Old issues, new threats

- **Force Majeure –** Increasing severe weather incidents, terrorist attacks
- **Legacy modernization –** Cutover issues, system crashes, corrupt data
- **Cyber attacks –** Denial of service, ransom ware



Business Continuity Planning is the key

Business Continuity Planning (BCP), Continuity of Operations Plan (COOP) and IT Disaster Recovery (ITDR) are critical to minimize business disruption and negative impact on client services in times of crisis.

Key components include:

- Evaluation of risk
- Business impact analysis
- Coordination and management to recover technology & operations

Questions you need to ask yourself:

- When was the last time you **updated your BCP**?
- Are you **prepared for a cyber attack**?
- How does cloud fit into your **ITDR strategy**?

New technology = New risks

Cloud, mobility, connected vehicles, modern systems –
As jurisdictions become more reliant on technology, they should plan on how to operate when its not there!

How can jurisdictions stay on top of these changes?

- Conduct vulnerability assessments of state-wide networks, systems and data. Identify exposures and define mitigation strategies
  - Emphasis is on maintaining the plan; implementing protection methods; training, testing, and exercising; and mitigating risks.
  - Technology can help by providing remote means to collaborate, test & train.

3 Key areas of focus

- **New technology & new business continuity planning assumptions**
- **Rethinking IT disaster recovery**
- **Review of emergency & incident management plans**

New technology -> New BCP assumptions

- **Each operational unit must constantly asses the impact of new technology:**
  - Will the recovery times be modified?
  - Will the unique requirements affecting operations be adequate?
  - Is there a process to restore essential functions?
  - What is the agency depending on and what if its not there?
- **Identify procedures, priorities, and resources (personnel, facilities and equipment):**
  - Which tools will improve the ability to continue operations?
- **Identify an alternate work area:**
  - Which mobile communication options (e.g. hotspots and portable equipment) can be used to continue operations?

Rethinking IT disaster recovery

IT DR plan and cloud technology will require reassessment of risks, timelines and procedures

- **Update risk plan to reflect the new risks introduced**
- **Re-align services and protocols**
  - Update recovery timelines and procedures
  - Update routing tables, IP addresses, VPN, web portals
  - Well defined outage scenarios, situation and assumptions
- **Network communications - availability**
  - Alternative recovery points, redundancy and out of band
- **Alternate locations - Cloud, regional/internal or hybrid**

Emergency & incident management

- **Emergency/Incident response operations**
  - Test interoperability with other agencies in a unified command structure
  - Link agencies together using common protocols
- **Identifying an alternate work area**
  - Include mobile communication options such as hotspots and portable equipment
  - Develop basic equipment lists
  - Work from home provisions
  - Define workarounds
- **Communication Plan - Communication paths, reports, schedules, interoperability**
  - Automate employee notification
  - Setup shared work areas using tools such as SharePoint

Checklist to ensure business continuity

- **Develop teams** that are charged with **periodic reviews** of Disaster Recovery, Continuity of Operations and Emergency Management
- **Refresh** in order to take advantage of the business process improvements and service delivery efficiencies that come with **advances in the technology**
- **Complete an updated list** of all Agency staff with contact information and summary of individual skills
- Keep the contact list of **Agency Business Partners** and third party service providers **updated**

New **technology provides enabling tools**;
It's the **people** who **make them work**

Contact information

For More Information Contact:

Nicholas Demetriades

Senior Principal, Infosys Public Services

Nicholas.Demetriades@infosys.com

860 9674 830