Security Imperatives in Your BC/DR Strategy

Disaster Happens, Now What?

- What is your immediate and natural reaction?
  - Need to get critical business processes back up and running as fast as possible
  - Need to get employees back to work
  - Need to avoid costly downtime
- Security is often the least considered, if not last consideration when responding to these situations.

Avoid the Double Whammy!

- Overlooking data protection provisions in our Business Continuity and Disaster Recovery
  - Can lead to not only a recovery scenario needing to be exercised, but…
  - A security breach
- Remember compliance isn't lifted in an emergency!

So What's the Playbook?

- Business agreement is critical
  - Make sure alignment is in lock step with businesses desires.
- Data classification levels
  - Not everything is critical.
  - Make sure you identify the order in which systems and/or data should be made available.
- Establishment of Recovery Point Objectives (RPO)
- Establishment of Recovery Time Objectives (RTO)

Things to Consider

- Security is just as important for BC/DR site as it is for primary production site.
- During a disaster should security concerns be heightened?
  - Some more than others?
  - Don’t let your guard down.
- Security controls will be different for different types of data.
  - But again should be similar to primary site.
- Active/Active vs. Active/Passive

To Cloud or not to Cloud???

- Cloud gives us many options and a perceived flexibility, but consider this…
  - What indemnification clauses are in the agreements?
  - Are background checks done?
  - Security controls should be similar to primary site.
- Active/Active vs. Active/Passive
  - Consider the different costs

Multi-Tenancy

- Multi-tenancy depends on the demark points
  - What services are shared?
  - Sharing of network is a common one so consideration is key.
  - What security protocols are in place to ensure it?
- How are those contracts vetted?
  - Who establishes priority?

So You Have a Plan, Now What?

- First step in testing BC/DR is testing your restore.
  - Connectivity should be tested frequently.
  - This includes making sure contracts are in place (Telecommunications, Cloud, etc.).
- Documentation and procedures need to stay current.
  - Want to prevent it from getting stale so quarterly checks to make sure data is still good should be the norm.
  - People turnover, people get busy and forget to document changes, or just plain get too busy for documentation of changes due to urgent issues.

So Everything is OK now, right?

- There is one law that is constant. Murphy's Law!
- What happens if things don't come up? Then what?
  - Is there a manual alternative to providing services?
  - What security protocols should be adhered to?

Questions???