In Case of Emergency:
Break Glass

A look at BCP, DRP, & Digital Legacy

David Bell - @dtbell91
david@bell.id.au

Sebastian Terfloth CC-BY-SA-2.5

~$ whoami

- David Bell
- @dtbell91
- david@bell.id.au
- SysAdmin/Spam Ninja at MailGuard
- Previously: 3 years Infrastructure Team @ Treasury Corporation of Victoria
- Attended: lca2012, 2014, 2015, 2017
- Conference Director: lca2016
- Linux Australia Council 2017

Treasury Corporation of Victoria

- Central financing authority for the State of Victoria
- Interface between State Authorities and wholesale finance market
- Issues Australia Government backed bonds domestically and internationally
- Works to maintain Victoria’s AAA/Aaa rating
- Manages $AU30bn-$AU50bn in State debt

Disclaimer

- This isn’t a horror story
- I’m here to talk to you about the exciting topics of:
  - Process
  - Testing
  - Backups
  - Documentation
- This advice is of a general nature, your circumstances may differ.

Talk Overview

- ~~Who am I?~~
- ~~Who is TCV?~~
- ~~Disclaimer~~
- Definitions
- Why?
- Creating your BCP
- Testing
- Culture
- ‘Breaking the glass’
- Personal application

Definitions

- BCP – Business Continuity Plan:
  - A process of creating systems (physically and process) to prevent and recover from Business Interruption Events
- Business Interruption Event:
  - Events which could interrupt the normal flow of your day-to-day operations
- DRP – Disaster Recovery Plan:
  - A plan for the recovery from a declared disaster following a catastrophic Business Interruption Event

Definitions

- RPO – Recovery Point Objective:
  - A targeted recovery point
- RTO – Recovery Time Objective:
  - A targeted recovery time frame
- Digital Legacy:
  - Person digital artifacts and accounts

Why?

- Because things will go wrong
- Possibly very wrong
- Because things shouldn’t have to get even more wrong

Creating your BCP

- Brainstorm
  - What are your business’ deliverables
  - What do you require to achieve these
  - Assign weights

Creating your BCP

- Identify the types of events which might impact
  - Loss of (access to) physical site
    - PT interruptions, protests/civil unrest, service outage
  - Loss of (access to) virtual site/DC
    - Network interruptions, “The Cloud”, “The Cybers”
  - Loss of staff

Creating your BCP

- Identify what you need to recover from an event
  - Physical hardware
  - Virtual resources
  - Backups
    - 3 copies of your data
    - 2 different media/formats
    - 1 offsite & offline
  - Data entry/transfer from BCP systems

Creating your BCP

- Authority
- Decide early, document decisions, and communicate
- Communication chains
  - Platforms?
  - Contact details?
  - Phone tree?

Testing

- Practice early, practice often
- Test real scenarios
- Measure, measure, measure
- Record your results

Testing

- Convert your results into action items
- Regression test
- Book your next BCP test
- Test early; test often
    - Once every quarter

Culture

- BCP isn’t owned by IT; IT is just an enabler
- Each Business Unit should have their own BCP
- Talk to the business
- Build in resiliency, work on good UX
- Have known good restore points

- Did I mention testing often?

Disaster Recovery

- Tested backups – an untested backup might be completely useless
- Documented restore and recovery processes
  - In what order do your services need to be brought up?
- Recovery is costly, know what your insurance will cover and try to avoid

Breaking the Glass

- In-house IT is unavailable
- No time/opportunity for handover
- Worst case scenario

Breaking the Glass

- Documentation is key
  - As built documents
  - Support playbooks
  - Vendor contacts
  - Credentials
- Secure credential storage is super important
- But how do you securely handover those keys?

Shamir’s Secret Sharing

- Divide a ‘secret’ into a number of ‘shares’
- Require a predefined quorum of ‘shares’ to recreate the original ‘secret’
- *quorum - 1* is useless to an adversary

- Various libraries and tools exist to generate/rejoin shares

Breaking the Glass

1. Place a copy of your encrypted password store (e.g. KeePass) in a tamper evident envelope in a secure location/escrow
2. Encrypt the passphrase for the password store using a new GPG key
3. Put the encrypted passphrase in a second tamper evident envelope at the same location

Breaking the Glass

4. Shamir’s Secret Sharing is used to generate ‘shares’ for each Director/Board Member/Exec Team member

5.Each share is placed in a tamper evident envelope with a complete set of instructions for their use

Breaking the Glass

6. Regularly review the validity of the tamper seals and destory (and recreate) remaining shares if a breach/loss is detected

7. If a complete breach is suspected commence a password change process

You have a password change process, right?

Digital Legacy

- Great, my employer can go on without me, but what about my systems/data/services/accounts/cat pictures?

- In essence, the same applies
  - Document
  - Backups (tested backups!)
  - Shamir’s Secret Sharing

Digital Legacy

- Document
  - Credentials (in KeePass or similar)
  - Services (hosting, domain names, cloudy cloud)
    - What uses them
    - Billing arrangements
    - Credentials
  - Your wishes for the above
  - Talk to your family and friends
    - Bonus points if you can convince them to do the same!

Digital Legacy

- Backups
  - 3 copies, 2 media/formats, 1 offsite/offline
  - Encrypted
    - Don’t forget to backup your encryption key as well somewhere else!
  - Personal data (photos, emails)
  - System configurations
    - Bonus points if you’re using Config Management in source control!
  - Documented
  - Tested!

Digital Legacy

- Shamir’s Secret Sharing
  - Applied the same as for your employer
  - Distributed tamper evident shares to your family and friends that you trust
  - Offer to do the same in return
  - Useful if you lose access yourself!

Review

- Creating your BCP
  - Business deliverables and requirements
  - Reviewed types of events
  - Communication and authority
  - Testing, measuring, regression testing
  - Culture
- Disaster Recovery
  - Test your backups
  - Document your recovery processes

Review

- Breaking the Glass
  - Documentation
  - Secure credential storage
  - Shamir’s Secret Sharing
- Digital Legacy
  - Documentation
  - Backups
  - Shamir’s Secret Sharing

Questions?
Discussion?
War stories?