

# Lions and Tigers and Bears, Oh My!

Adam Backman – Head Punkhawallah

White Star Software



**White Star**  
software

# About White Star Software

- The oldest and most respected independent Progress OpenEdge consulting firm
- The top OpenEdge DBAs in the world
- Our performance, monitoring and alerting tool, ProTop. An incredibly powerful single-pane-of-glass view of your entire OpenEdge ecosystems
- Mentoring and skills transfer from real world DBAs

[info@wss.com](mailto:info@wss.com) | [wss.com](http://wss.com)



# About Adam Backman

- Worked for Progress when there were only 80 employees worldwide (Yes, he is old)
- Wrote a book for Progress Software about database administration and OpenEdge management
- Loves solving problems with a focus on the operation of the business



# Recovery planning

- We will discuss
  - Who
  - What
  - Where
  - When
  - Why
- Of recovery planning

# Why do recovery planning?

- The best answer is: So it works when you need it
- To establish an understanding of what is possible
- To define what you care about and what you don't
- To eliminate second guessing after the fact
- To look to the outside world as if business is as usual

# Home of the Carona virus and excellent planning

---



# Security

- Perceived security
  - This is how you feel
- Actual security
  - This is what will actually work
- Both are important but it is important to understand the difference

# Lucky person?

---





Now what do you see?

---



# Who do you involve in the planning phase

- Be inclusive
- You don't own the data the users own the data
- People to involve
  - End users
  - Management – you need funding
  - Technical people – multiple silos
  - More people can provide a complete view of your environment

# Who is responsible

- For backup
- For recovery
- For decision making during recovery
- For contacting people
  - Status reporting during incident
  - Contacting staff after major incident

# What is important?

- High probability risks
- High impact risks
- High cost risks

# Sources of problems

- Human errors
- More human errors (really)
- Application code
- Hardware/software system failures
- Man-made disasters
- Natural disasters

# The REAL source of system problems

---



# High impact issues

- Loss of environment
  - Fire may only impact a portion of the building
  - Earthquake may impact entire region
- Loss of infrastructure
  - Network
  - Client machines
  - Phones
  - Chairs

# Cost impact of downtime

- Cost of lost business
- Cost of additional employee time
- Cost to rekey/lost data
- Cost to switch to other (manual) system
- Cost to reputation



# Don't worry about things that are unlikely to happen

- People in Hawaii really don't need to worry about blizzards
- People on the east coast don't really need to worry about earthquakes
- Zombie Apocalypse



# Don't build a solution that costs more than the problem

- This underscores the importance of knowing the cost of downtime
- A daily backup is fine for many businesses
- Using after imaging is cheap and easy to archive off site frequently
- Some people need a second set of hardware with replication to keep downtime to a minimum

# Cost of solution vs. probability of problem

The lesser of two weevils



# Building a good recovery plan

- Create your plans based on recovery
- Do not focus on the process until the end
- Understand the cost of losing each portion of your business and infrastructure
- Recovery planning is way more than just data

# What to include in your planning

- Data
- Application(s)
- Hardware
  - Compute
  - Network
  - Client machines
  - Phones and other supporting hardware
- What happens if you lose a/the building

# Creating recovery plans

- Focus on the likelihood of the issue
- Most common failures first
- Not having to recover is always best
- Humans are always the weak link so start there
  - Deletion of files/database
  - Security for the system (internal and external threats)

# Eliminate the human element

- Automation of all tasks
- Reporting on all outcomes
- Alerting on all variances

# Eliminate the human element

---



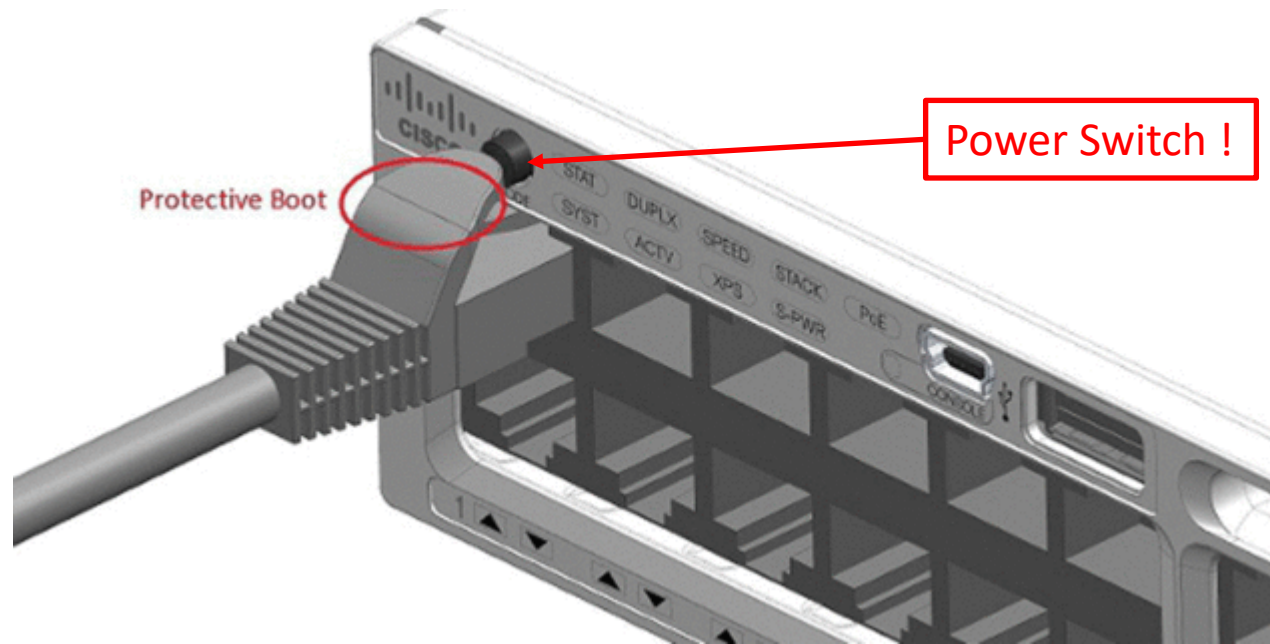


# Building reliable solutions (software)

- Standards
  - Naming standards
  - Source code control
- Standard release process
  - Separate development, test and production environments
- Testing
  - Manual and automated testing

# Importance of peer review

---



# Where?

- Where does the backup go?
  - Second machine – where?
  - Tape – then where?
- Where is the replica machine?
- Where do people go if there building is not there?
- Where is the backup hardware?

# When?

- When to backup
- When to try a workaround
- When to recover
- When to test your recovery plan

# Building a good recovery plan

- Who – involve many in the initial planning
- What – remember that your application is more than just data and application code
- Where – second sites or the cloud can act as repositories for your backups/AIs/replica DBs
- When – full backup daily and test at least annually
- Why – look to the outside world as if nothing is wrong

Questions?



**White Star**  
software