Risks, Disasters – And Your Career

Lessons from Y2K, Business Continuity, and Incident Response

David Soubly,
Chief Squirrel Herder
Skybird Creations, LLC

Warmup

https://theneedlefish.com/2021/10/16/great-movie-scenes-china-syndrome-turbine-trip/

https://www.youtube.com/watch?v=nemYBeT4aQY

About Me

- Principal, Information and Cyber Security – ICEX (Intellectual Capital EXchange)
- Ford IT Manager – SecOps, Strategy, Audit, Business Continuity, Large-Scale Systems Support, Production Control, Availability, Large-Scale Data Center Planning
- Writer – Long / Short Fiction, Poetry, Essays
  - See www.davidsoubly.com/blog
- Pianist / Composer ("Endurance: Stories for Our Times")
- Woodworker / Gardener / Fiber Arts Creator / Hiker

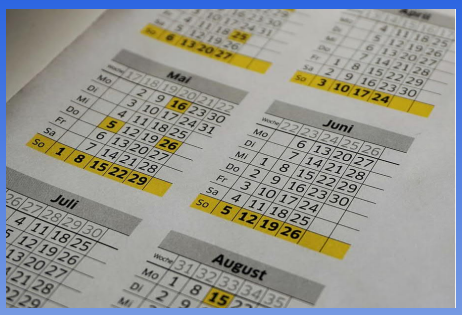
Life's Too Short
To Be
A One-Trick Pony

Topics for Today

- Y2K – A Fable, Revisited
- Business Continuity – A Perspective
- Incident Response – When You Stand In the Fire
- Responsibilities As Auditors / Cyber Security / Risk Professionals / Fraud Examiners
- What This Means for Our Careers – the Three "Ps"

Y2K – A Fable

- Once Upon a Time…
- How the Problem Grew
- Implications
- What Should Be Done?
- A Bias for Action: Making the Unknown Known



https://www.davidsoubly.com/blog/post/the-y2k-fable

Skybird

- Once upon a time…
  - Far fewer computers, limited storage space
  - Languages like COBOL, Fortran, PL/I and databases like Oracle and IBM
  - Huge amounts of mainframe data that today would fit on an external drive
  - Space, processing time and retrieval efficiency were all a premium
  - Dates stored in YY format
- How the problem grew
  - Accretion over time – thousands of decisions
  - Lack of documentation, “developing” programming disciplines
  - An early indication of technical debt
- Implications and Choices
  - What happens at millennium rollover
  - Where is the problem buried?
- What should be done?
  - Opinions: Everything, nothing, or something in between?
- Bias for Action
  - Make the unknown known
  - Consequences of looking the other way
  - The implied penalty of under-reacting

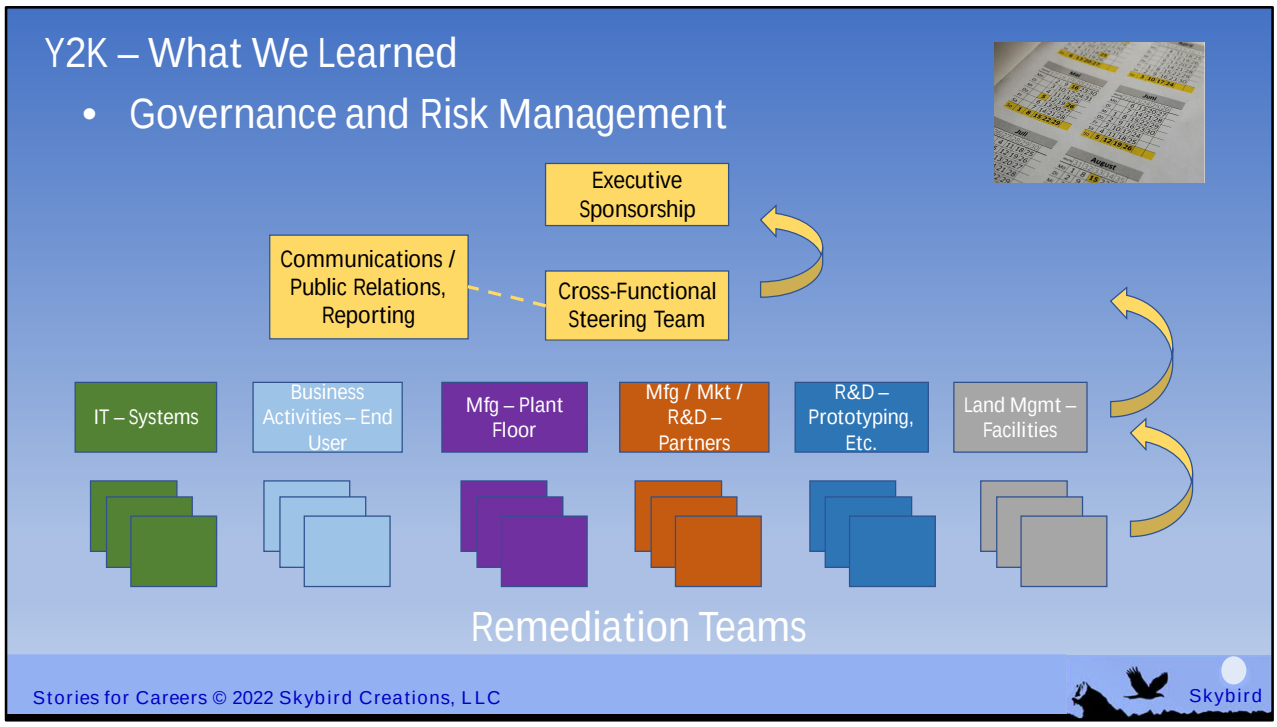
Y2K – What We Learned

- Making the Unknown Known: "Cover the Card" Approach

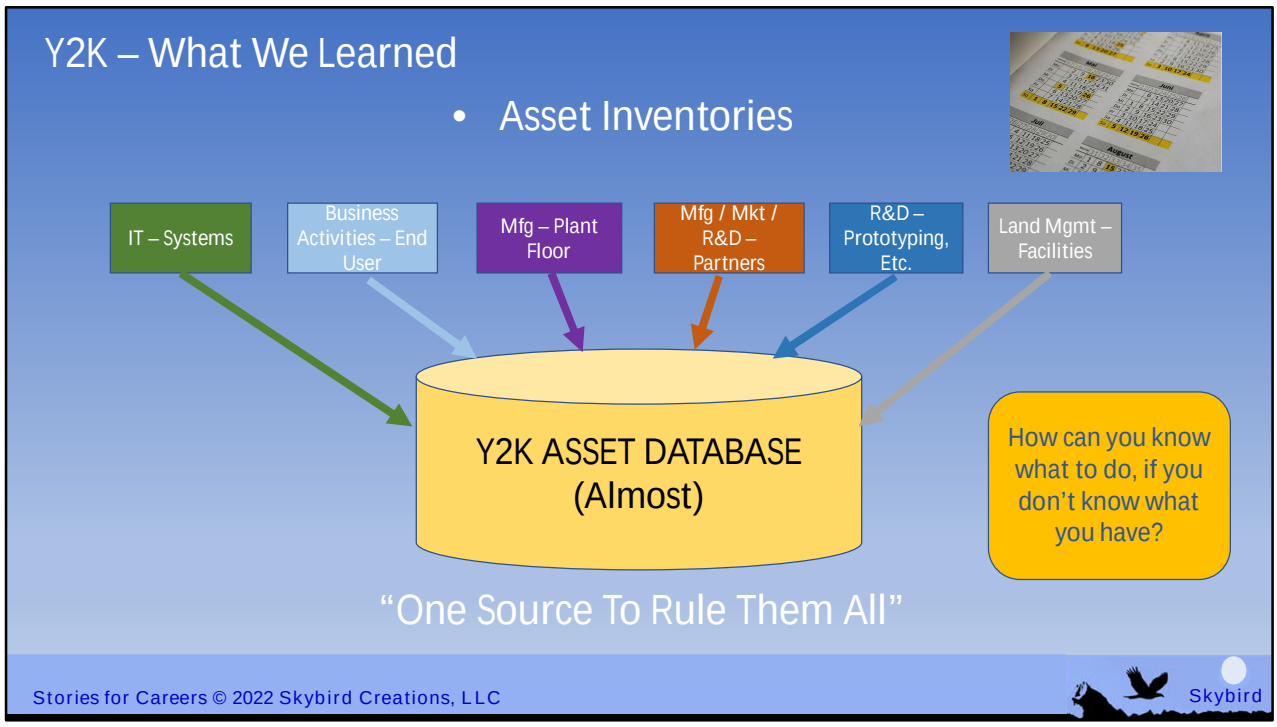
Business Area	Process Steps					
System Code	Identify	Prioritize	Remediate	Test	Implement	Document
End-User						
Plant Floor						
Partnerships						
R&D						
Facilities						

Skybird

- "Cover the Card"
  - Whole-business view; extended business
  - 550 million lines of COBOL code; 2 billion lines of PL/I
  - Hundreds of thousands of endpoints
  - Plant Floor - Programmable Logic Controllers – (aside on Stuxnet); probably the first time we'd encountered the IT / OT situation
  - Dealers, suppliers, affiliates – fast forward to supply chain issues today
  - R&D – prototyping
  - Facilities – building controls
  - Today we would add cloud, IoT, IIoT, mobile devices, augmented reality – but these are all essentially variations

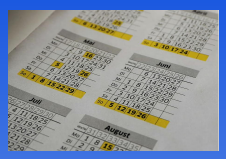


- GRC
  - Importance of executive sponsorship / messaging, from the business
  - Cross-functional executive team to steer the effort
  - Downward arrows of delegation and control I'm not showing to keep things simple
  - Various activities reported up progress, issues (upward arrows)
  - Communications / PR / Reporting – for external consumption



- Importance of Asset Management
  - Essential for crisis management
  - How can you know what to do, if you don't know what you have?
  - Reducing the fog of war in any situation requires knowing what you have
  - What constitutes an asset
  - Who "owns" the Asset Database
  - The "almost" – Plant Floor did their own thing

Y2K – What We Learned

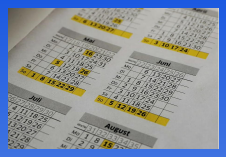


- Politics and Perspectives
- Opportunities, Opportunists, and Opposition
- What an Anti-Climax Feels Like
- Missed opportunities

Skybird

- Politics and Perspectives
  - Big problem / no problem
  - Business problem / IT problem / Not my problem
- Three O's
  - Opportunity – establish fundamental inventory; factory approach; renovate code
  - Opportunists – snake-oil salesmen vs honest partners; hype (planes fall out of sky)
  - Opposition – business, political
- Anti-Climax
  - Five minutes to midnight
  - Five minutes after midnight
- Triage
  - Knowing ahead of time what the most critical, most at-risk areas – essential for business continuity
  - Minimize amount of disruption
  - Some areas might have been bypassed or "done last," for good reason

Y2K – What Did We REALLY Learn?



- 20+ Years Later ("Y2K22" "Log4J" "Break the Internet")
- Who Was Right?
- The Truth About Truth
- The Truth About Us - Biases
- Implications for Today – Reinforcements, Echo Chambers
- Implications for 20 Years from Now: What Will We Know?
- The Vital Role of Auditors, Cyber Security, Risk and Fraud Professionals
- Landing in Fact

SAIPAN

www.davidsoubly.com/blog/post/saipan

Skybird

- 20 years later, we still have date-based minor issues – Y2K22 affected some exchange servers
- Far more challenging – vulnerabilities like Log4J and attacks like Solar Winds
- Who was right – we'll never know
- Truth is elusive – refer to "Saipan" – WWII – U.S. and Japan – Citizen suicides
- Truth about us – we form opinions early and seek reinforcement (note about biases built into AI – colleague's remarks around ethnicity and gender vs other bias markers – bias is individual)
- In today's world, our views are sharpened by social media and reinforced by echo chambers
- 20 years from now, all we'll know about COVID is what we did, and where we presently are
- We will never know which course of action would have been the best
- Why this story? Auditors present unwelcome news; must gather evidence; land in fact

Y2K – Implications for Auditors, Cyber Security and Risk Professionals

- Landing in Fact
- What is Fact?
- Evidence, Conclusions, Presentations, Repercussions
- Wicked or Stupid – Is It That Simple?
- Rationalizations and Evasions
- Expediency, Speed, Tradeoffs, and the Like
- Do the best we can, as truth is rare and elusive

Skybird

- What does it mean to land in fact?
- Work hard at assembling evidence, drawing conclusions, presenting findings
- Be prepared for repercussions
- For auditors, wicked or stupid?
- For fraud, rationalization, opportunity – they already know they're doing wrong
- Fraud triangle – Wall Street Titans – Boesky and Dennis Levine, his insider trader
- Some more likely to not care than others

Business Continuity – Some Examples

- Business Continuity and Disaster Recovery
- But what IS “Disaster Recovery?”
- Popular Examples

https://www.davidsoubly.com/blog/post/a-mistake-any-of-us-could-mak

Skybird

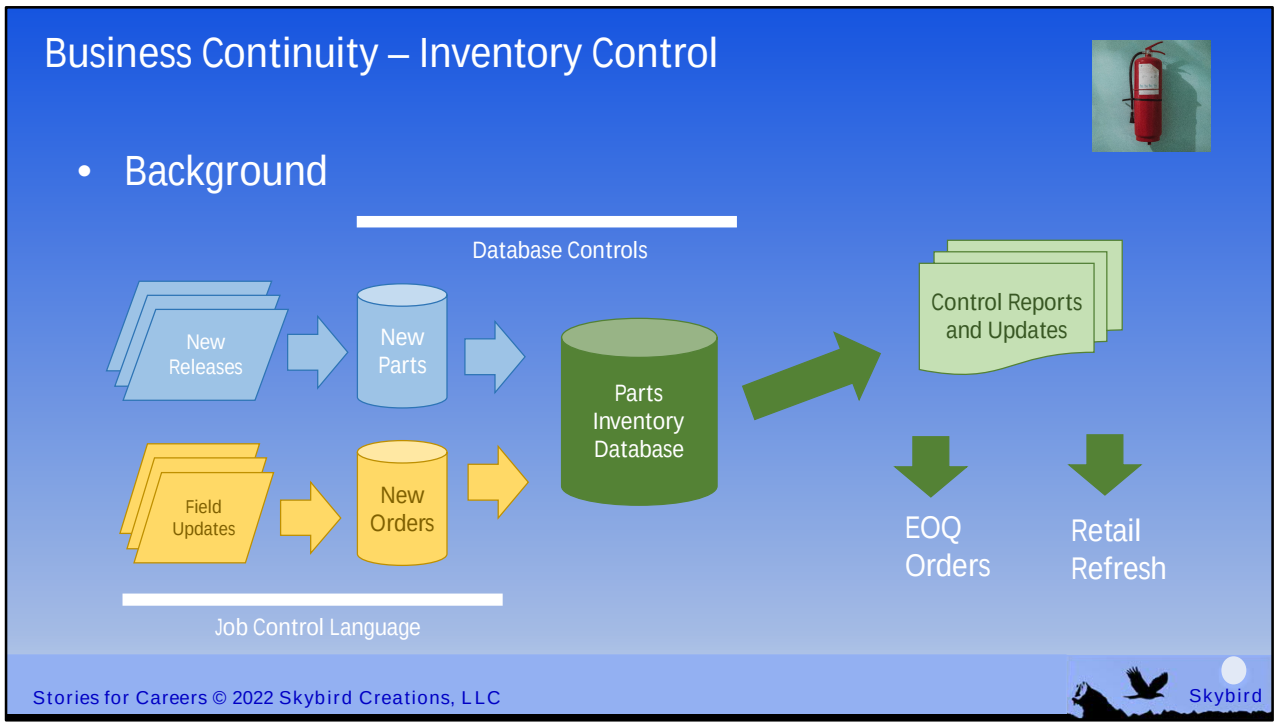
- What’s the difference between business continuity and disaster recovery

Business Continuity – Inventory Control

- Background
- The Problem
- The Fix
- The New Problem
- The Incubation
- The Impact
- The Fallout
- The Lessons Learned

Skybird

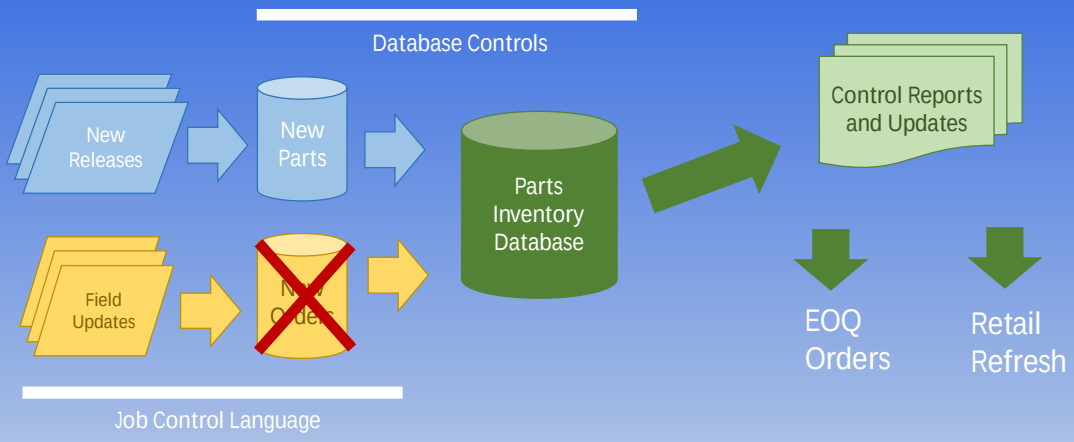
- Summary of discussion



- Picture inventory control system
- New parts released into the system by engineers
- Hundreds of thousands of new orders from retail outlets across the country
- Numerous inputs to update master database
- Updates generate reports, EOQs, shipments, etc.
- Traditional mainframe – JCL, IBM MVS, IMS

Business Continuity – Inventory Control

- The Problem

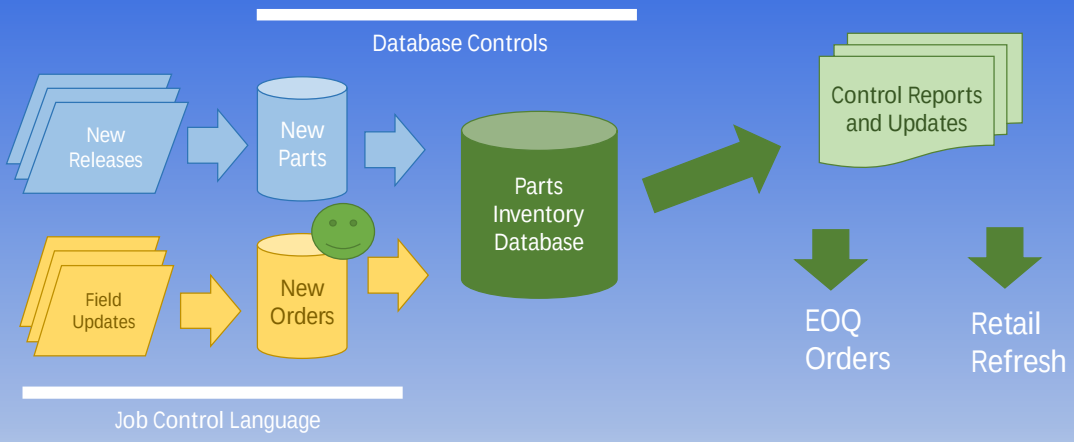


Skybird

- Programmer, 2am, support call – come in and fix
- New parts order database is down
- Program or input issue
- Analysis required

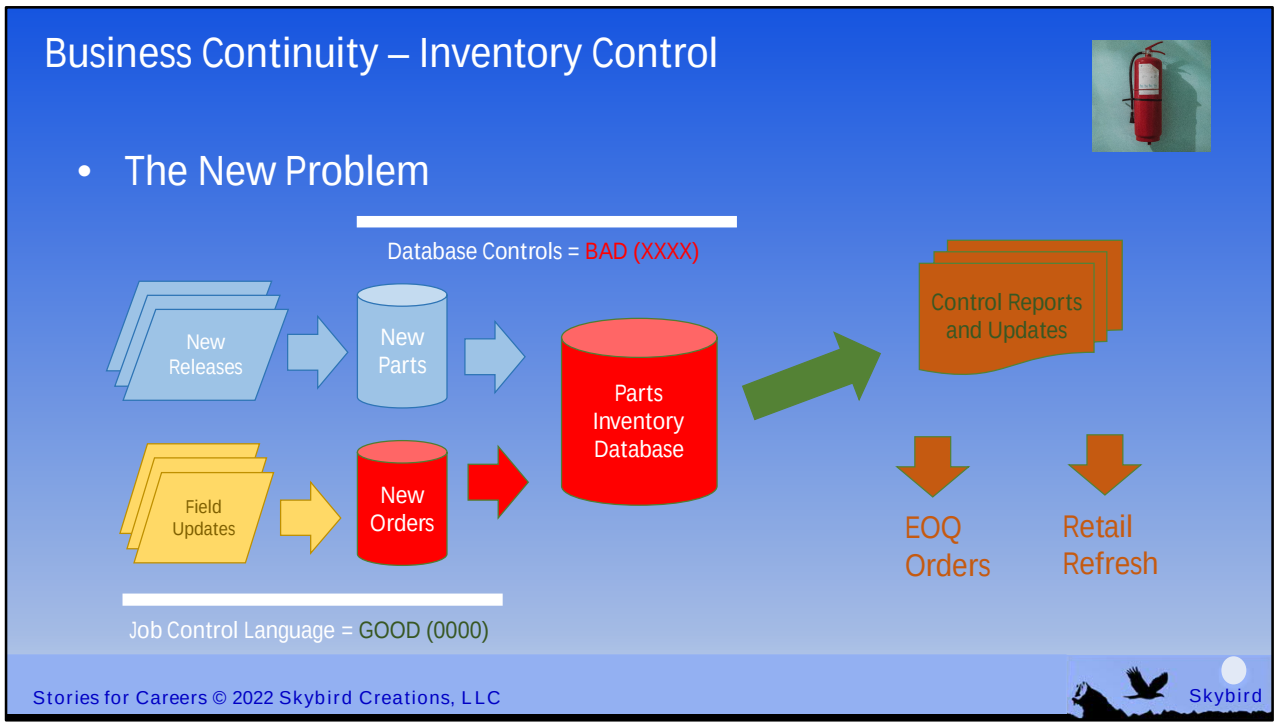
Business Continuity – Inventory Control

- The Fix

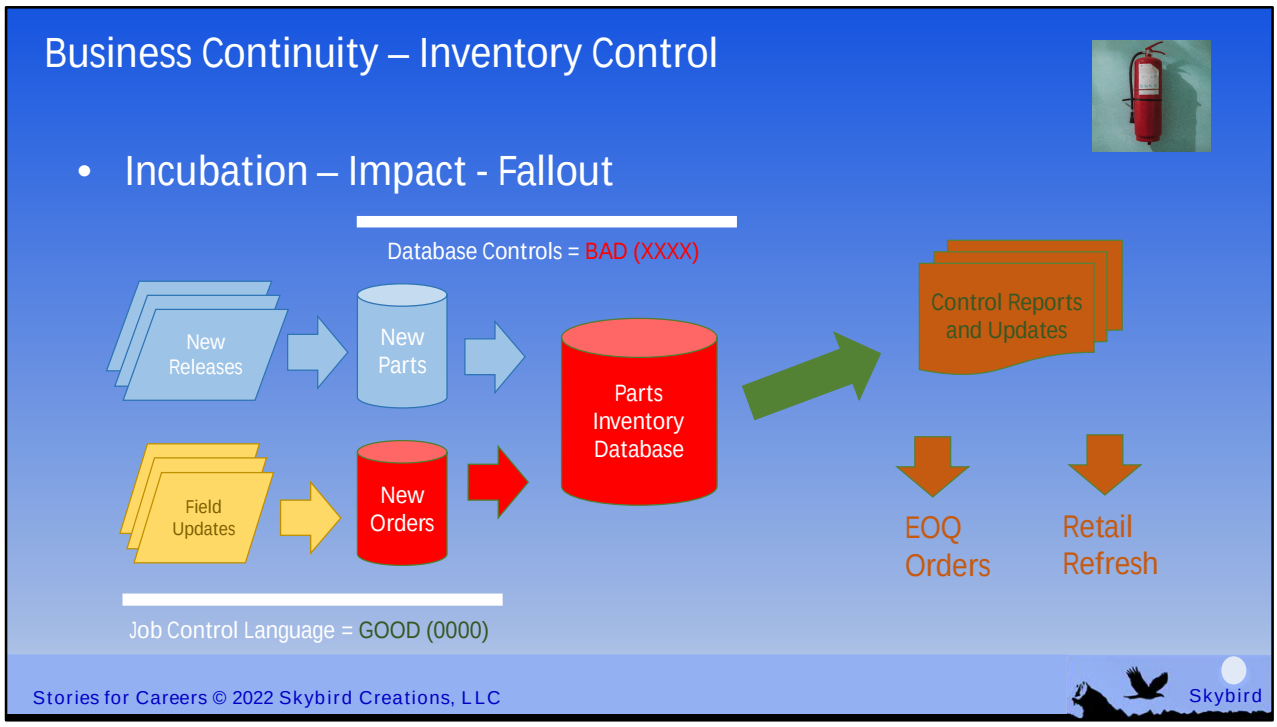


Skybird

- Programmer assesses situation
- Quick fix
- Authorizes manual startup of jobs
- Checks that job completed successfully
- Things look good, goes home, goes to bed



- Problem
- Program fixed, job run; condition codes checked; all ok; run next job; programmer goes home
- Issue – did not check database condition codes; jobs ran ok but databases were not properly updated
- Wrong inventory position for thousands of parts – which ones, who knew



- Wrong inventory position for thousands of parts – which ones, who knew
- Incubation – not noticed for about a week
- First signs of trouble; then escalation; then realization
- Inventory positions are not known with certainty for any parts across any warehouse, all over the country
- Logs not available; emergency management meetings daily and on weekends
- Potential – count every part manually; months of effort; huge cost; no new development; men / women worried about their jobs
- Happy ending: information discovered, applied; system rescued
- After-action – revisions to job completion procedures; checks / balances, etc.

Business Continuity – Other Examples

- Brown's Ferry – A Lighted Candle

http://www.ccnr.org/browns_ferry.html

- Dresden – A Faulty Gauge

https://en.wikipedia.org/wiki/Dresden_Generating_Station

- Lake Peigneur – A Fourteen-Inch Drill

How One Engineer's Tiny Mistake Made An Entire Louisiana Lake Completely Disappear

- ROOT CAUSES

Skybird

- This and next example are from earlier nuclear industry
- Not picking on this industry, but these happen to be
- Fixing air leaks, cable spreading room, nuclear control facility
- Candle – Fire - Attempts to put out themselves -Things not working
- Fire affects controls, condition of reactor unknown (liken this to 747 flying to London; halfway there, no instruments)
- Fire department finally called; identifies type of fire; puts it out
- Fallout – almost a nuclear incident
- Lessons – follow procedures; call in professionals
- Dresden Power Generating Station (Inspiration for China Syndrome)
    - Faulty gauge, downstream errors, decisions, have to fight to control reactor for a couple of hours
- Lake Peigneur – shallow lake became deep saltwater lake – Texaco – Diamond Salt Mine

Business Continuity – What Did We REALLY Learn?

- Little Cat Feet
- Slow Motion "explosions"
- Preparedness
- Attention to Detail
  - Sweat the Small Stuff

The fog comes
on little cat **feet.**

It sits looking
over harbor **and city**
on silent haunches
and then moves **on.**

-- "Fog", **Carl Sandburg**

Stories for Careers © 2022 Skybird Creations, LLC

Skybird

- Business disasters creep in
- Some may be slow-motion
  - Examples – chip shortage – result of supply chain decisions, single points of failure, switching challenges
    - Root cause might be from many individual low-cost decisions resulting in paring down supply change redundancy
    - Failure to see the big picture
    - Failure to understand what your most critical assembly components may be and planning contingencies
    - "Explosion" – can no longer produce most popular products
  - Examples – Stock bubbles – everything from Tulipomania to 2008 – knowing you're in a bubble but unable to stop
    - Sudden "explosion" that was really long in coming
  - Examples – Wells Fargo
    - Designed-in ethical failures
    - Reinforced by management and making the numbers
    - Resulted in cross-selling and opening accounts with no knowledge by consumer
    - "Explosion" was when this came to light
- Preparedness is tough – harder to stay awake than to fall asleep
  - How can you know when you're hollowing out your supply chain
  - How can you know when a stock market run-up is actually a bubble
  - How can you know when the data reported to you on new credit applications is based on fraud?
- Attention to detail – Rescorla and Sept 11 – Sweat the small stuff

Incident Response – The Worm Attack

- The Backstory
- The Situation
- The Information
- The Challenge
- The Decision
- The Result

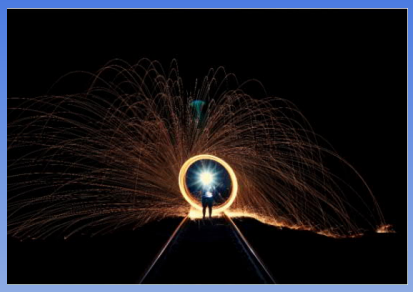
https://www.infoworld.com/article/2677291/blaster-worm-spreading--experts-warn-of-attack.html

Skybird

- New CIRT supervisor
- Immediately prior – SQL Slammer paralyzed networks worldwide
- Great tech team – what was I doing leading them?
- CIRT Duty Analyst – pager – call to supervisor
- Honeymoon over – “Blaster” arrives during workweek
- 2,000 machines impacted, number growing
- Bridge call
- Arguments for severing connections to other regions
- Impact – real-time information flows
- What data? Attack numbers stable
- The decision: Hold; Assess; be ready to sever
- Result – Event averted; machines patched

Incident Response – The Worm Attack

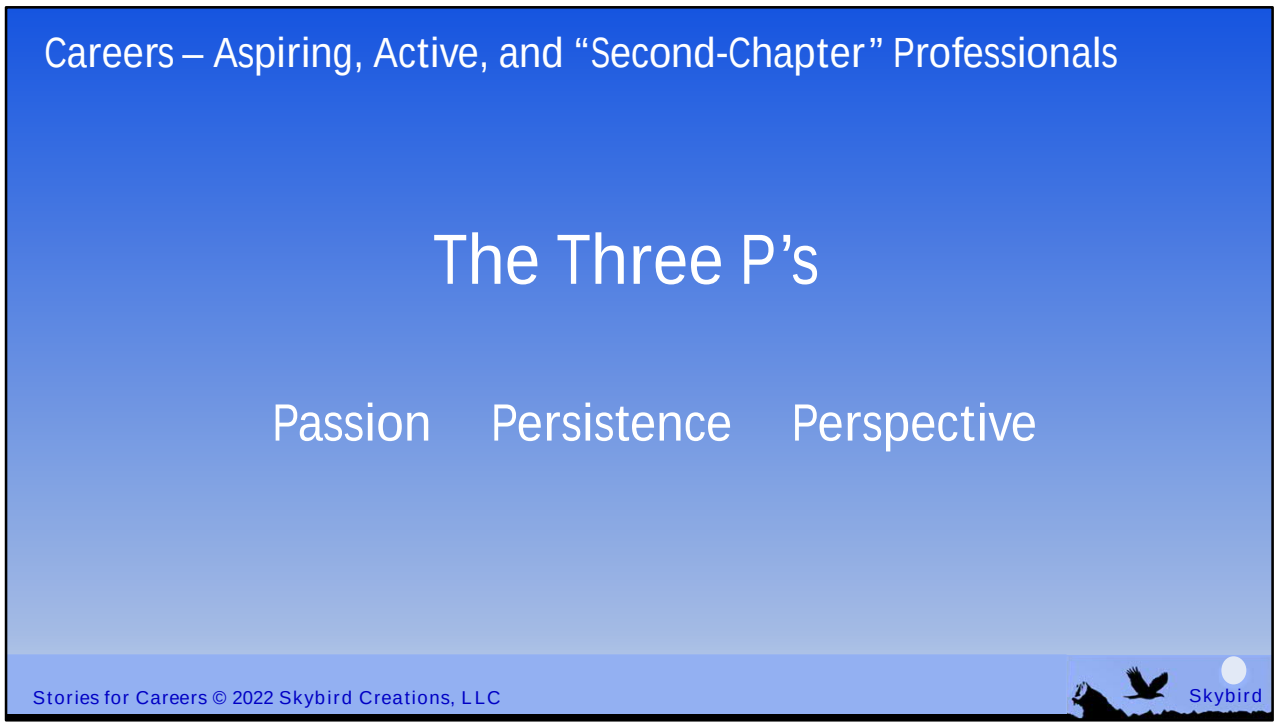
- Lessons Learned



https://www.davidsoubly.com/blog/post/standing-in-the-fir

Skybird

- Lessons learned – Stand in fire; wonderful team focus; data are never all in; critical decision must be made with best available data
- Confidence – best decision at the time
- A lot like strategy – finding a way forward as event unfolds
- Respect for first responders



- What does this teach us generally
- Something I call the three P's
- Passion – Persistence – Perspective
- Bring this to the work you do, or look for this when you hire

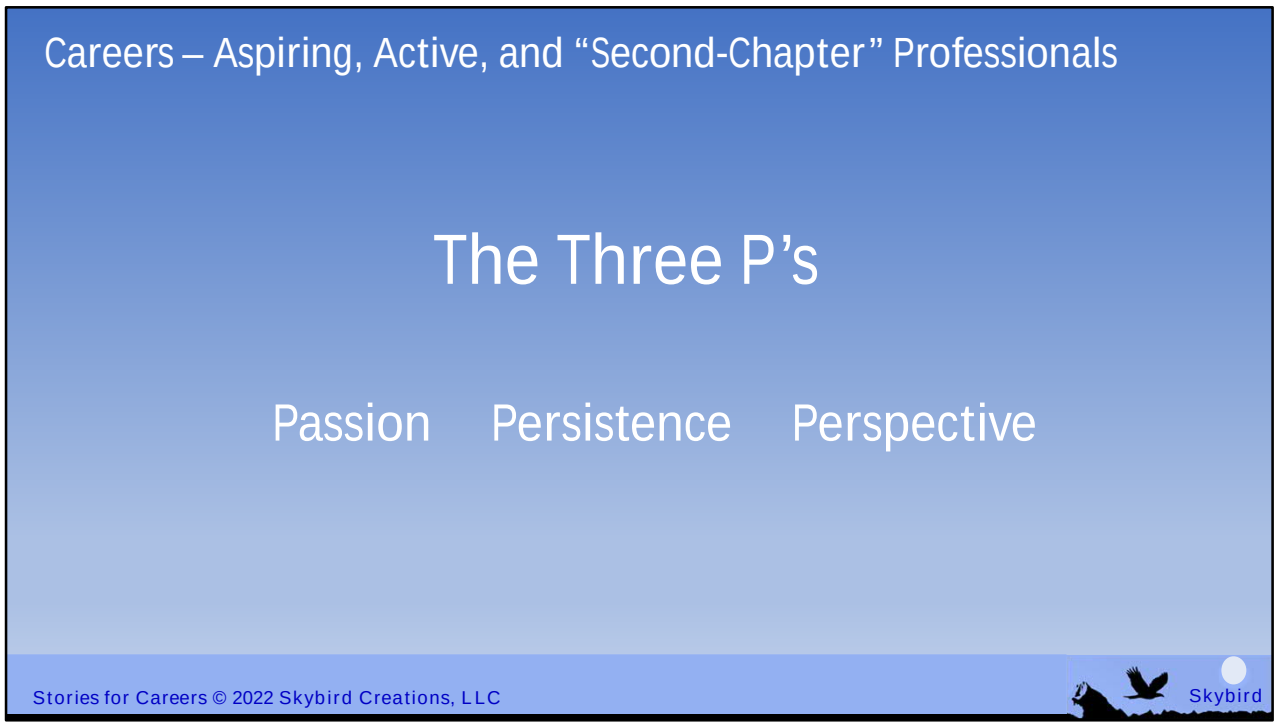
- Passion – drive – interest in what you're doing
- If you don't feel passion for the work, then assess - time to move on; could you be doing something else?
- Passion can ebb and flow; or it can fade
- Recruiting – "What gets you going in the morning?" Or – alternatively – "What keeps you up at night?"
- If you're interviewing or moving – ask yourself the same thing

Careers – We, As Professionals; We, As Aspiring Professionals

Persistence

- Manoj Bhargava – Passion, slapped; change passion
- Persistence is what really matters
- Bjorn Borg – Tennis ball over the net one more time than my opponent
- Churchill – going through hell – keep going
- Old saying – the harder I worked, the luckier I got
- How to recruit for it? Ask stories – "Tell about a time when you were disappointed; fell down; hit a wall; etc. – what did you do?"
- We all have stories – Don't be afraid to discuss what you learned through failure
- Famous story – person who blew a product and lost $100 million

- Mark Twain quote – Older I got, the smarter the old man seemed to be
- Richard Pryor – No such thing as an old fool – you don't get to be old bein' no fool
- What the examples I gave tonight teach is about perspective
- Without perspective, we can easily repeat problems of the past
- Perspective can't be a straight-jacket, though – beware of "always done it this way" trap
- Issue – we don't often hire for perspective – we hire for skills. But perspective may be the greatest skill of all.
- Recruiting for perspective – Conflict management question
- Recruiting for perspective – CIRT interview example



- Keep these in mind, moving through careers
- Keep these in mind, when looking for new recruits
- Remember also: to you, an experienced hire is really a new recruit – you're just taking a different kind of chance

Wrap-Up

"Aun aprendo" – "I am still learning"
-- Francisco Goya, Spanish Painter, 1746-1828

What Questions Do You Have?

Skybird

- As always, I'm still learning
- Questions – help me improve my understanding