



# Session 3120

## Best practices: Application uptime is no accident



**Ron LaPedis, CBCP, CISSP, ISSAP, N6QGK**  
**Sr. Product Manager**

© 2004 Hewlett-Packard Development Company, L.P.  
The information contained herein is subject to change without notice



# Agenda

- Information security
- Environmental review
- Business continuity





Information security

# Information security

- Key concepts
  - Encryption isn't only SSL
  - Identification, authentication, authorization, and privacy
- What does the Internet look like?
- Where do hackers come from?
- Priorities

# Security



## Encryption

- SSL—only protects business information from PC to Web server
- Record/file encryption—protects business information on the servers
- Communications encryption
  - End-to-end encryption
  - Line encryption
  - VPN/tunneling





# Identification, authentication, authorization, and privacy

- Identification—who you claim to be
- Authentication—who you really are
- Authorization—what you are allowed to access
- Privacy—what you should be allowed to access





# Identification, authentication, authorization, and privacy

- Proper user verification
- What business information goes online and who can access it?
- Interception of business information
- Hacking of business information—extortion  
Liability
- Phishing

# Authentication

- Multiple-use passwords are not secure
  - Can be given away or stolen
- Single-use passwords
  - Challenge/response
- System-assigned passwords are often written down
  - Password quality check is better
- What you **are**, what you **have**, what you **know**
  - **Biometrics**
  - **Token**
  - **PIN**



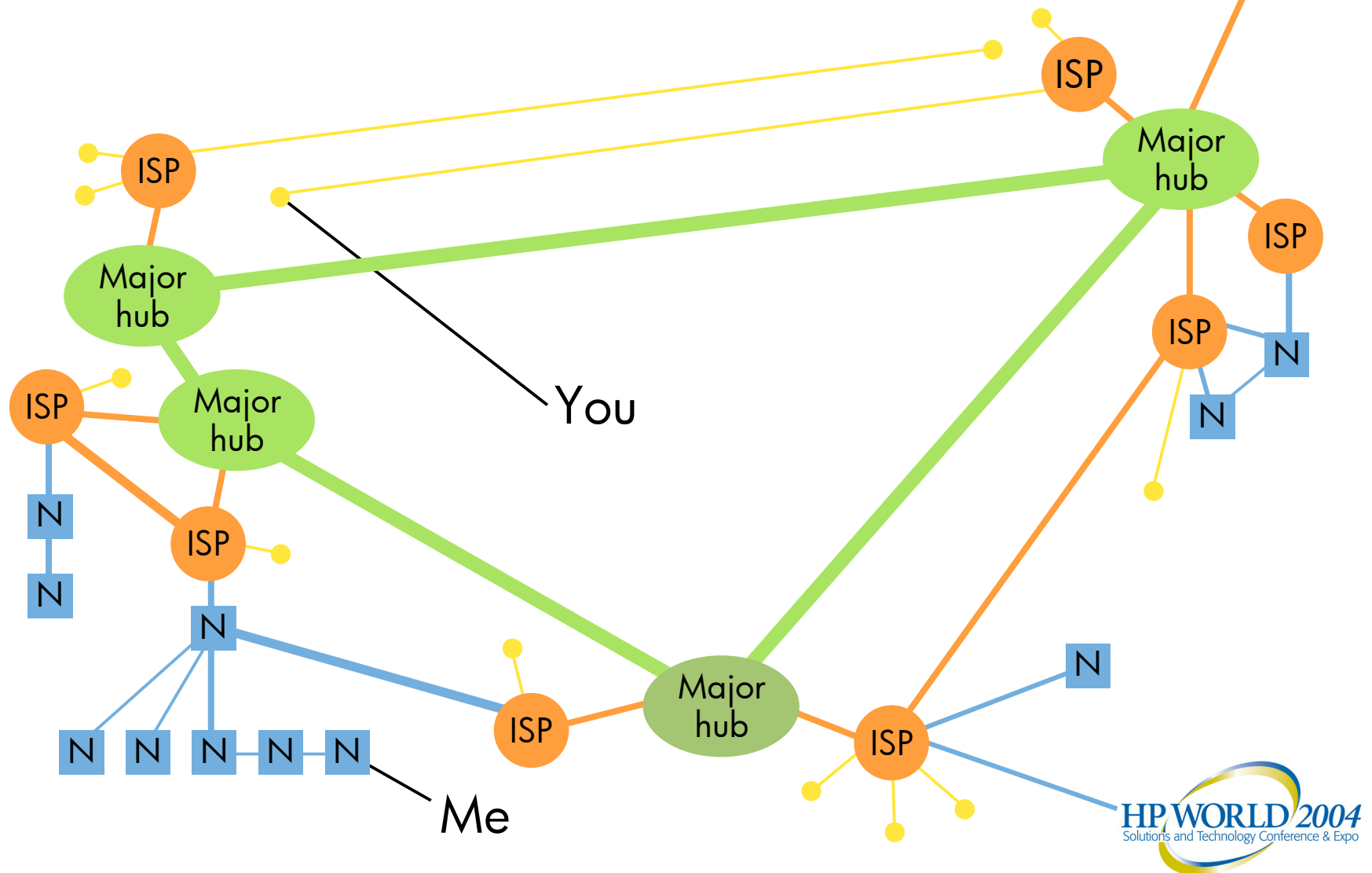
# Authorization

- Least privilege
- Role-based security
- Subject/object access control model
- Separation of duties

# Privacy

- Hot topic on the Internet
- Must flow from corporate policy
- Should be stated
- Your company's reputation relies on it
- Cookies
  - <http://www.junkbusters.com/ht/en/cookies.html>
- Web bugs
  - [http://www.eff.org/Privacy/Marketing/web\\_bug.html](http://www.eff.org/Privacy/Marketing/web_bug.html)
- Classification of business information and least privilege

# What does the Internet look like?



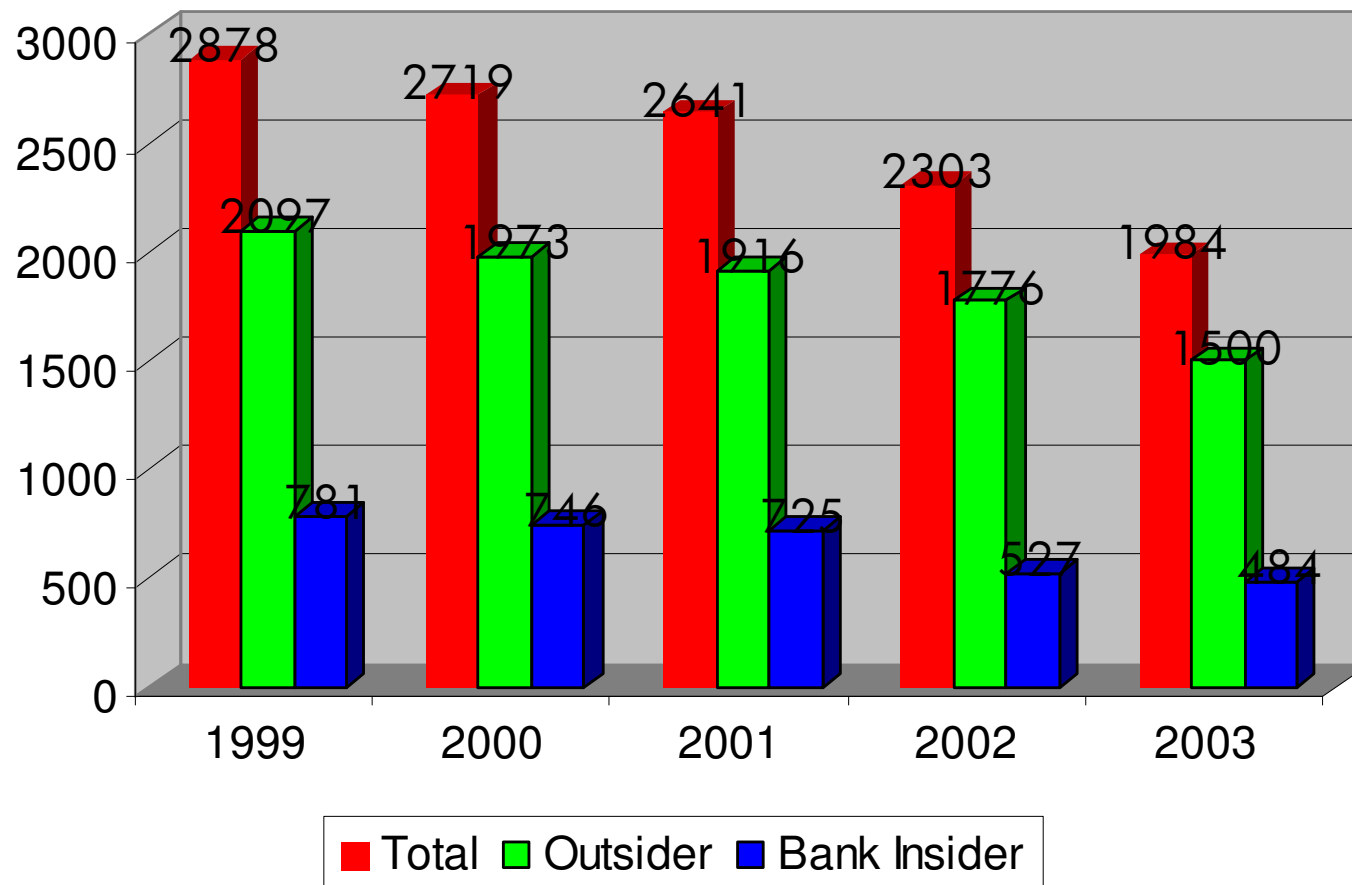
- Surveys say that most information security breaches come from insiders.
- Companies usually keep quiet about breaches, whether inside or outside.
- Most convictions are outsiders.



# Banking and financial institution security breaches

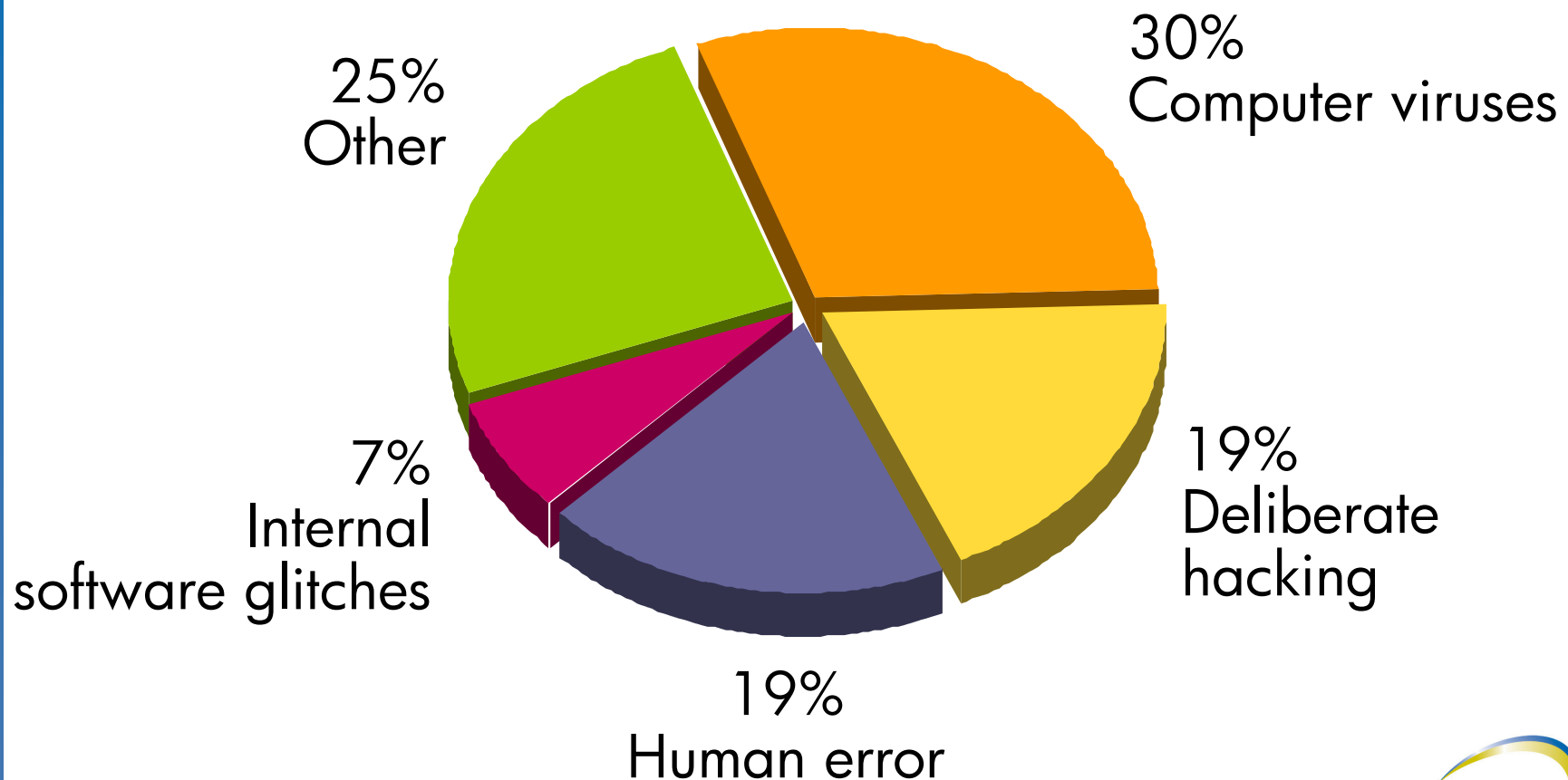


## Convictions - Outsiders vs Insiders



Source: FBI Financial institution fraud and failure report

# Banking and financial institution security breaches



Source: FBI 02/02



# Where do I start?

- Protect your systems from insiders first, then from the outside
  - Least privilege
  - Separation of duties
  - Quick deletion of terminated employee access
- Firewalls
- Encrypted databases, if necessary
- Multi-tier architecture
- Hardware key management

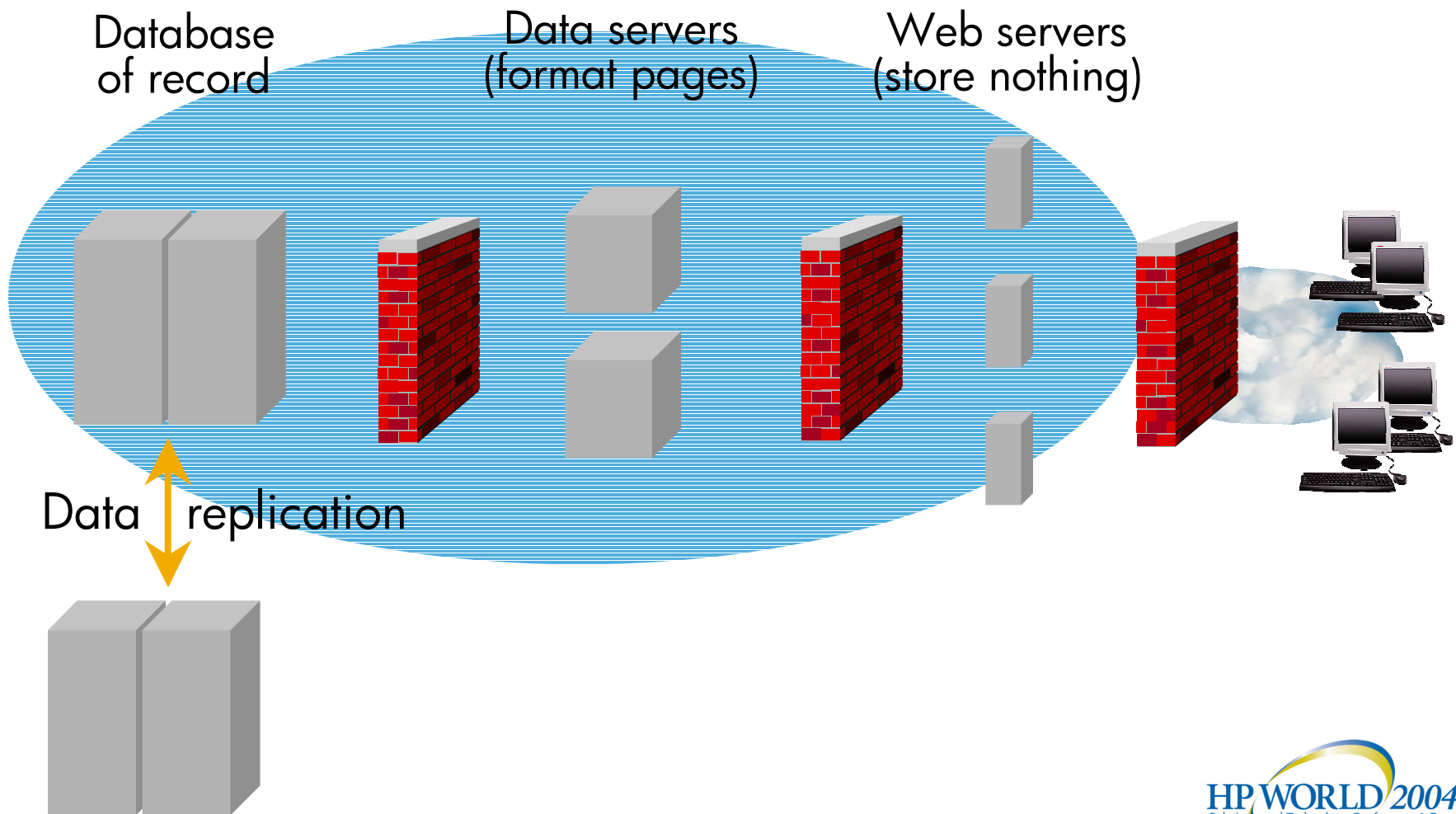
# Where do I start?

- Don't store anything on Web servers because they can be hacked.
- Subscribe to patch lists like bugtraq or CERT.
  - [www.securityfocus.com](http://www.securityfocus.com)
  - [cert.gov](http://cert.gov)
- Carefully evaluate the hardware and software you are using for inherent security.

# Multi-tier architecture

- Multi-tier infrastructure can help provide security.
- At each stage, use different ports or protocols to connect the systems.
  - The front end serves the pages.
  - The middle serves the data.
  - The database server protects the data.

# Multi-tier architecture



# Hardware key management

- Don't tempt even loyal employees.
- Overriding goal: there are never any keys "in the clear."
- No one sees or holds the complete "master" key.
  - Choose two (preferably more) trusted employees to hold key parts.
  - Choose from different departments to lessen possibility of collusion.
  - Combine key parts in a secure key injection device to create master.

# Hardware key management

- Encrypt all keys to be stored outside hardware security module (disk, cache, etc.).
  - Use a strong master key and a strong algorithm (like Triple-DES).
- Disable commands you don't use.
  - Weakest link is “common denominator” standards for interoperability with other systems.
- Work closely with product vendors.
  - Key management is an evolving science.



# Nov 2001: Triple DES attack published



- Insider attacks published by researchers at the University of Cambridge in the UK
  - IBM 4758 security module exposed Triple DES keys
  - Fourteen steps and approximately two days
  - IBM 4758 is validated at FIPS 140-1 Level Four!
  - The key point: Attacked Triple DES keys while at rest

**Atalla Labs has shared 14 separate attacks against Triple DES**



# Monitoring

- If you cannot detect intrusions, how do you know your security program is working?
  - Intrusion detection system (IDS)
  - Timely review of security logs (batch or real time)
  - Third-party IDS services

# If you are hacked

- Get the system off your network as soon as possible.
  - Possibly leave it connected to the Internet.
- Don't touch the computer unless you are skilled in forensic analysis.
- Do not power down the computer—what appears on the screen or in random access memory can be important.
- Get help if you need it.
- Get a bit-by-bit backup of the hard drives and archive the original drives for evidence.

# Why HP NonStop servers provide better protection



- Modular operating system
  - Except for a small kernel, most operating system functionality is handled by specialized system processes.
- Processes run in their own virtual address space
  - Communication is by messages; therefore, they cannot overwrite each other's memory.

No system is hack-proof, especially from insiders—  
always follow best practices.





Environmental review

# Dirty power

- The average number of outages sufficient to cause IT system malfunction per year at a typical site is approximately 15.
- 90% of the outages are less than 5 minutes in duration.
- 99% of the outages are less than 1 hour in duration.
- Total cumulative outage duration is approximately 100 minutes per year.

2002 American Power Conversion



# Environmental concerns for tomorrow

- Environmental problems and outages will increase as technology evolves.
  - Faster clock and processor speeds
  - Increased density of circuits for higher efficiency
  - Lower logic voltages to compensate for heat generation
  - Increased networking applications

# Two power cords for a reason

- Many servers have dual redundant power inputs, and most high availability data centers and network rooms take advantage of this feature to provide dual power path feeds to the server. These systems can survive a complete failure of any point in either power path and continue operation. During normal operation, the computers are designed so that power paths share the load.
- Each of the inputs should connect to separate outlets, panels, power distribution units (PDUs), feeds, entry panels, and energy sources.

# Professional services

- Comprehensive power audits and analysis
- Power monitoring
- RF and HF monitoring
- Grounding verification
- Engineering consulting
- Computer room design
- Lightning protection consulting



# Introduction to continuity planning

Based on the DRI  
International Certification  
Program



# Agenda

- Continuity planning? I thought it was called disaster recovery.
- Why?
- Professional practices
- Continuity planning activities
- Step by step
- Horror stories
- Food for thought



# Some people never learn...

November 30, 1989

## Crane collapse closes buildings

### Race for Rolodexes At Barricaded Highrises

By Diane Curtis  
Chronicle Staff Writer

Tennis shoes tightly laced, This is a time to put things in per  
shopping bags in both hands, spective."

...for 10 minutes...her job was to race through work areas and scoop up appointment books, payroll records, and Rolodexes needed to carry on business elsewhere...

main concern  
checks for em-  
ounting on their  
pages.

the most pre-  
phone lists and  
re rarely accord-  
to-day business.  
ostpone appoint

runner for several  
ing offices in the  
Building at 601 C  
Her job was to race  
areas and scoop u  
books, payroll rec  
exes needed to ca  
elsewhere while the firms wait for  
repair work on the damaged build-  
ing.

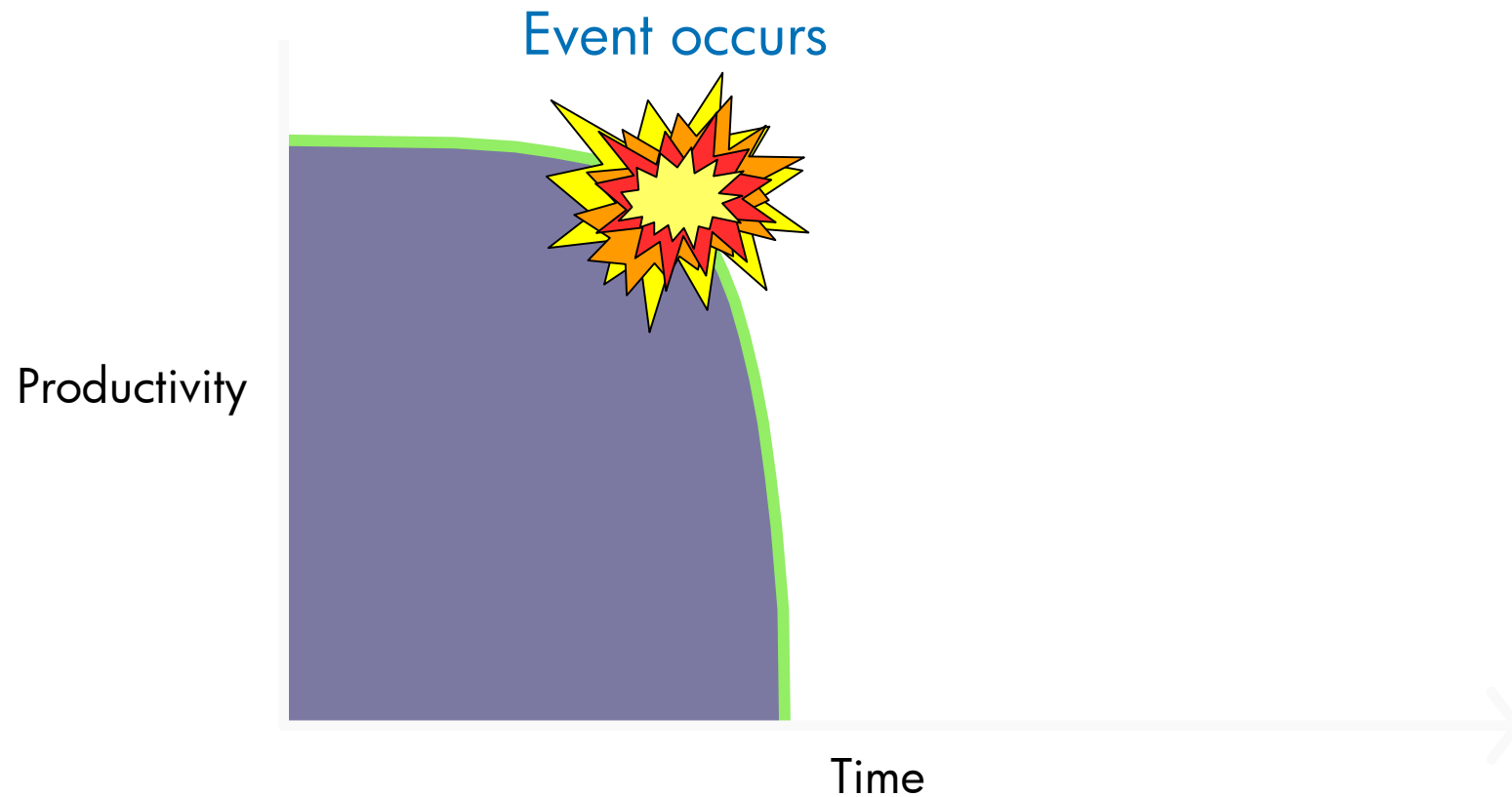
Many tenants' main concern  
was getting payroll checks ...  
phone lists and calendars

Francisco has a lot of resilience. It  
bounces back."

Source: San Francisco Chronicle

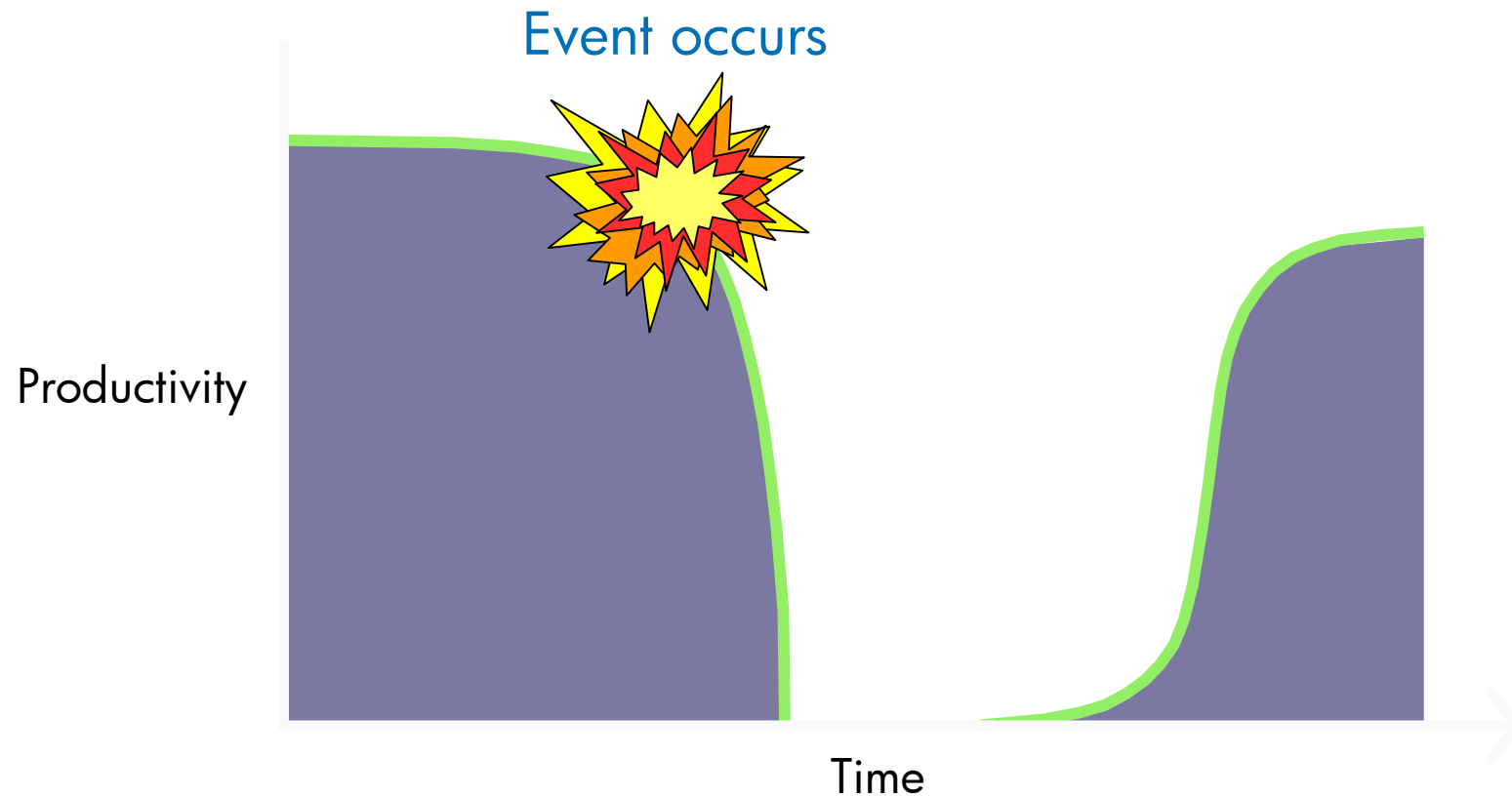


# Something happens



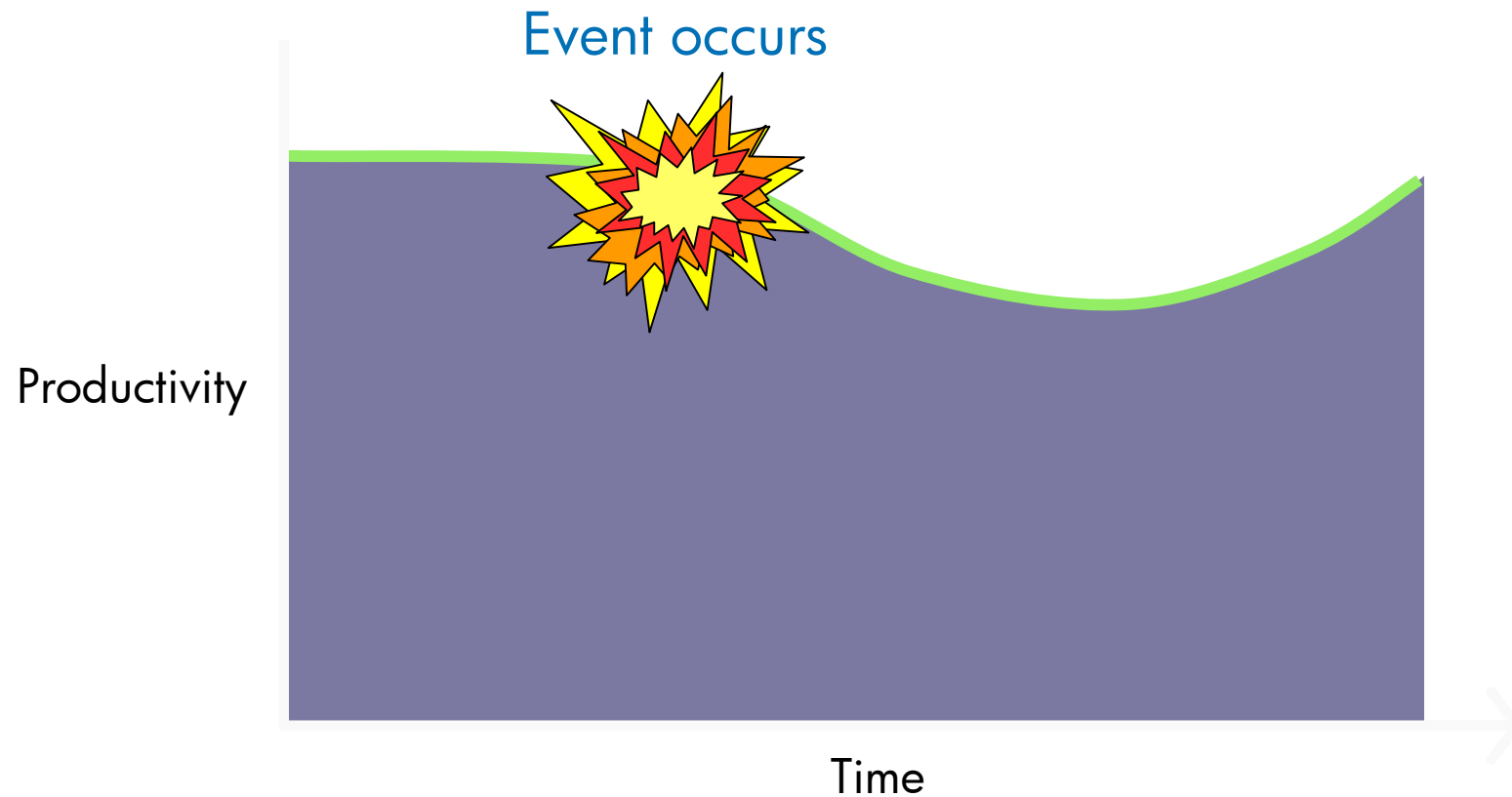
Source: DRII

# Disaster recovery



Source: DRII

# Business continuity



Source: DRII

# Why?



# Downtime is not acceptable

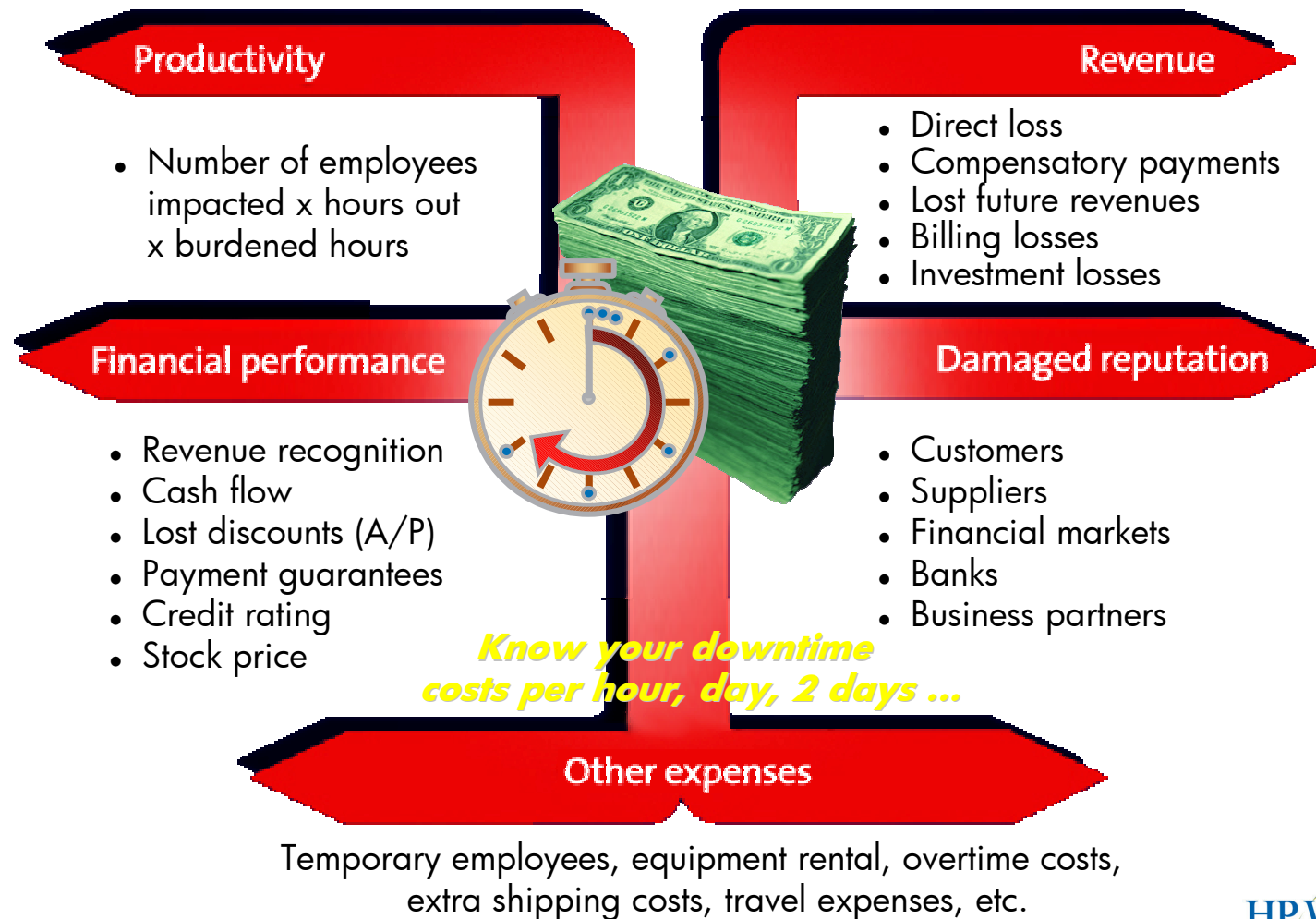
- Time zones are no longer a barrier to conducting business.
- If your site is down, your competition is one click away.
  - Utility failure
  - Communications failure
  - System failure
  - Application failure
  - Operating system failure
  - Utility upgrade
  - Communications upgrade
  - System upgrade
  - Application upgrade
  - Operating system upgrade

And what about  
system and  
database  
maintenance?

# What is your cost of downtime?

Industry sector	Rev/hour	Rev/emp. hour
Energy	US\$2,817,846	US\$569.20
Telecommunications	2,066,245	186.98
Manufacturing	1,610,654	134.24
Financial institutions	1,495,134	1,079.89
Information technology	1,344,461	184.03
Insurance	1,202,444	370.92
Retail	1,107,274	244.37
Pharmaceuticals	1,082,252	167.53
Banking	996,802	130.52
Chemicals	704,101	194.53
Transportation	668,586	107.78
Utilities	643,250	380.94
Healthcare	636,030	142.58
Professional services	532,510	99.59
Media	340,432	119.74
Hospitality and travel	330,654	38.62
<b>Average:</b>	<b>US\$1,010,536</b>	<b>US\$205.55</b>

# What is your cost of downtime?



# Downtime is controllable

- System and network architecture
  - High-availability systems
  - Redundant network
  - Hardened primary site
  - Remote backup site
- Continuity planning
  - Knowing what you will do before you need to do it



# Continuity planning perspective

- Ensures that an event doesn't become a *disaster*
- Covers a broad spectrum of business and technology issues
- The key goal: required business process availability



# DRI International

## Mission

DRI International's mission is to provide the leadership and best practices that serve as a base of common knowledge for all business continuity and disaster recovery planners and organizations in the industry.



# DRI International

- This section presents the business continuity planning model and the “Professional Practices for Business Continuity Planners,” the body of knowledge in business continuity planning, which are copyrighted materials of DRI International.
- However, the individual activities shown during the rest of the presentation were developed by HP and are **not** endorsed by DRI International.

# DRI International professional practices



## Preplanning

1. Risk evaluation and control
2. Business impact analysis
3. Project initiation and management

## Planning

4. Developing business continuity strategies
5. Emergency response and operations
6. Developing and implementing business continuity plans

## Post-planning

7. Awareness and training programs
8. Maintaining and exercising business continuity plans
9. Public relations and crisis communication
10. Coordination with public authorities



# DRI International business continuity planning model

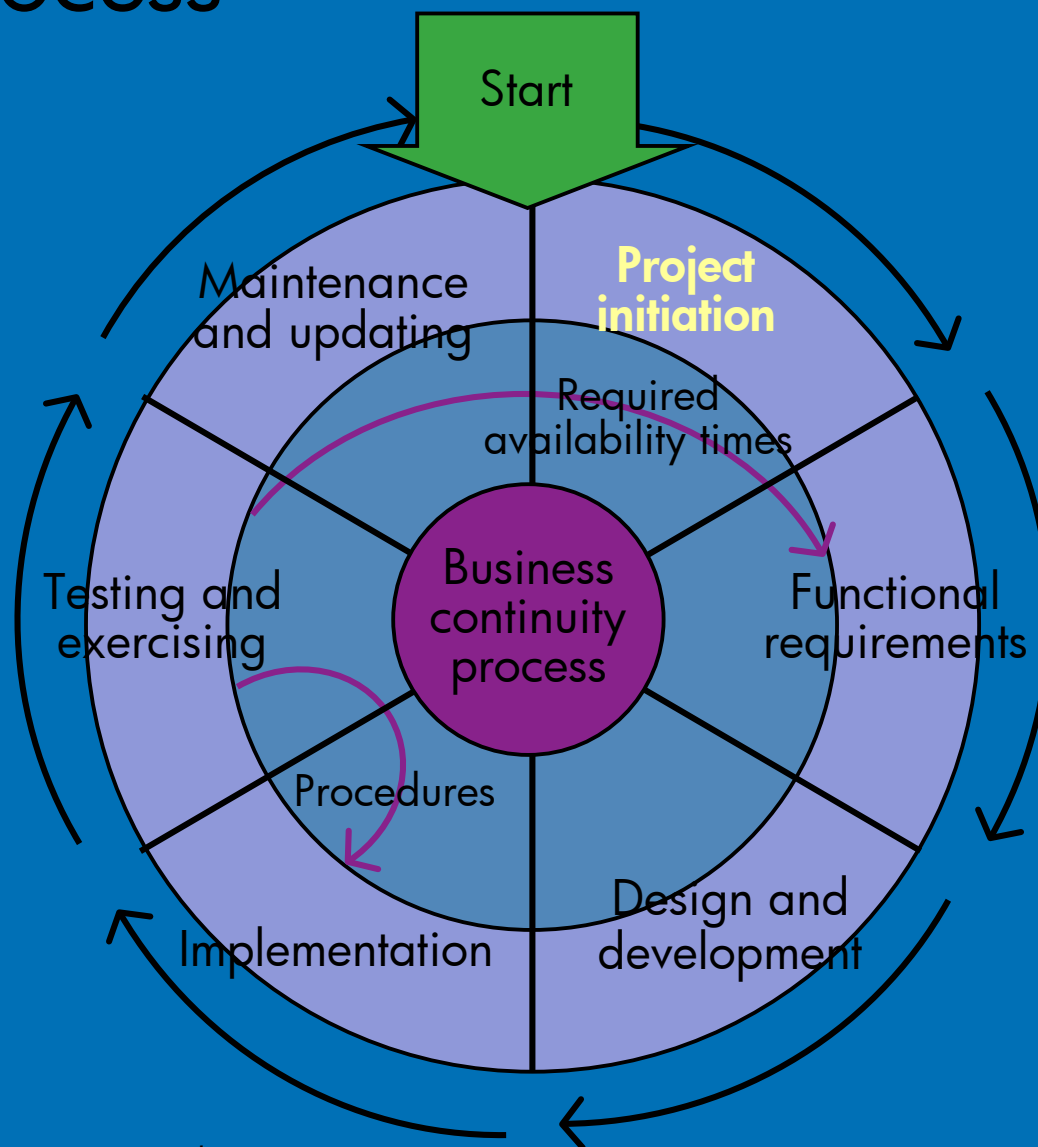


- Project initiation phase
- Functional requirements phase
- Design and development phase
- Implementation phase
- Testing and exercise phase
- Maintenance and update phase
- *Execution phase*

*Used by permission of DRI International*



# It's a process



# Project initiation phase

- Management commitment and policies
- Objectives and requirements
- Baseline assumptions
- Project management
- Corporate and business process teams

# Project initiation phase

- Management commitment and policies
  - Continuity planning must be considered a core activity and not an afterthought.
  - Just like security, continuity planning should be part of every business process.
    - “The management of XYZ company believes that continuity planning is key to this company’s survival and has committed the budget and resources to developing and maintaining a continuity planning program.”



# Project initiation phase

- Objectives and requirements
  - A real plan, not just on paper
  - Determining what is important to your business
  - Satisfying legal, regulatory, or other mandates
  - Planning for continuity, recovery, or both

# Project initiation phase

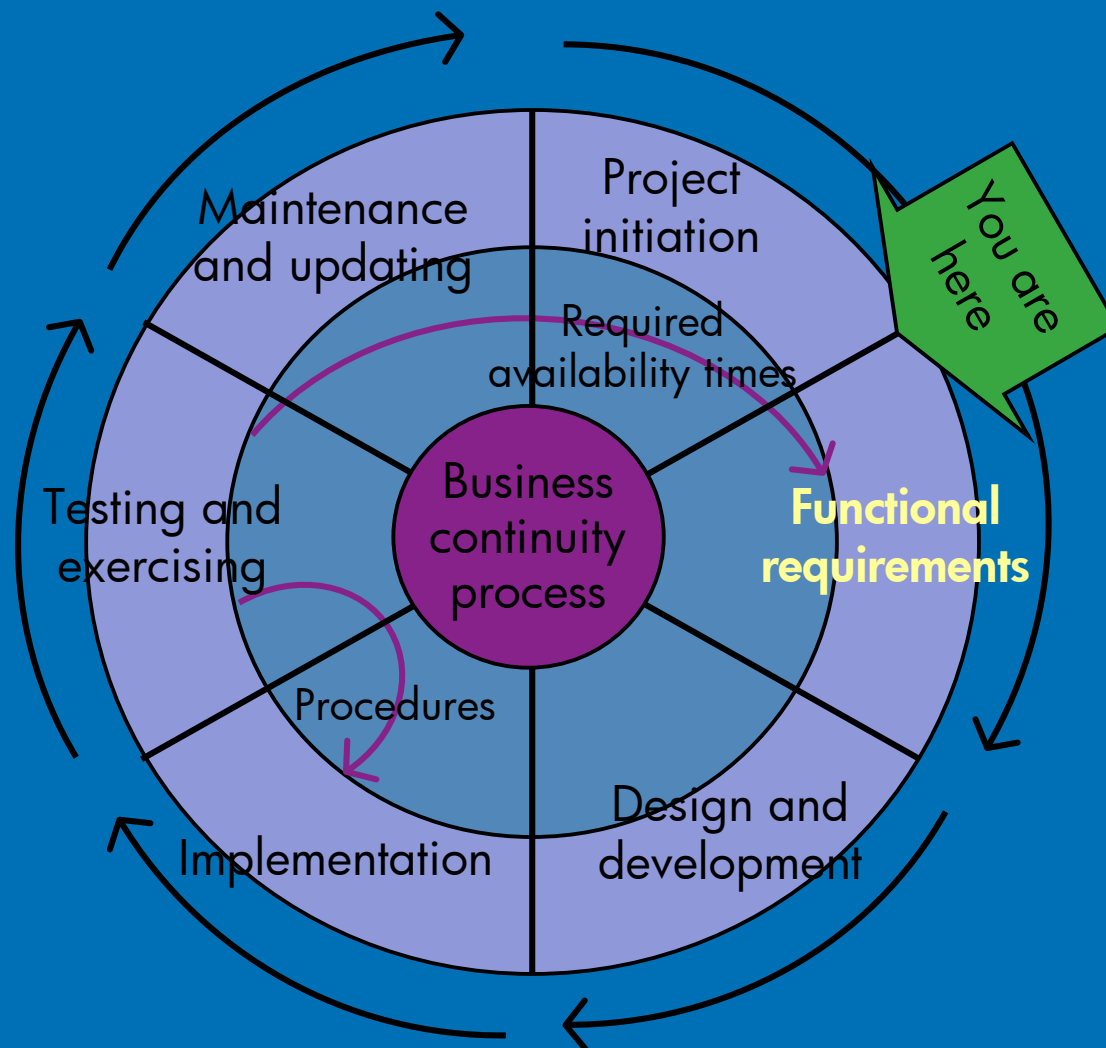
- Baseline assumptions—is there documentation for
  - Standard operating procedures
  - Run books
  - Data flow diagrams and problem isolation procedures (for business functions as well as computer applications)
  - Problem escalation
  - Change control process
  - Special forms and peripheral requirements
  - Data backup/rotation schedule

# Project initiation phase

- Project management
  - Continuity planning is a process consisting of programs and projects.
  - It does not take a subject matter expert to manage projects; it takes a project manager.
  - Use your continuity planning experts to perform continuity planning activities, not to manage projects.

# Project initiation phase

- Corporate and business process teams
  - Delphi—local to each key business function
  - Corporate team—supports business function recovery (after recovering themselves)
  - Emergency management team (EMT)—initial response and reports status to CMT
  - Crisis management team (CMT)—usually executive management—decides whether or not to declare a disaster

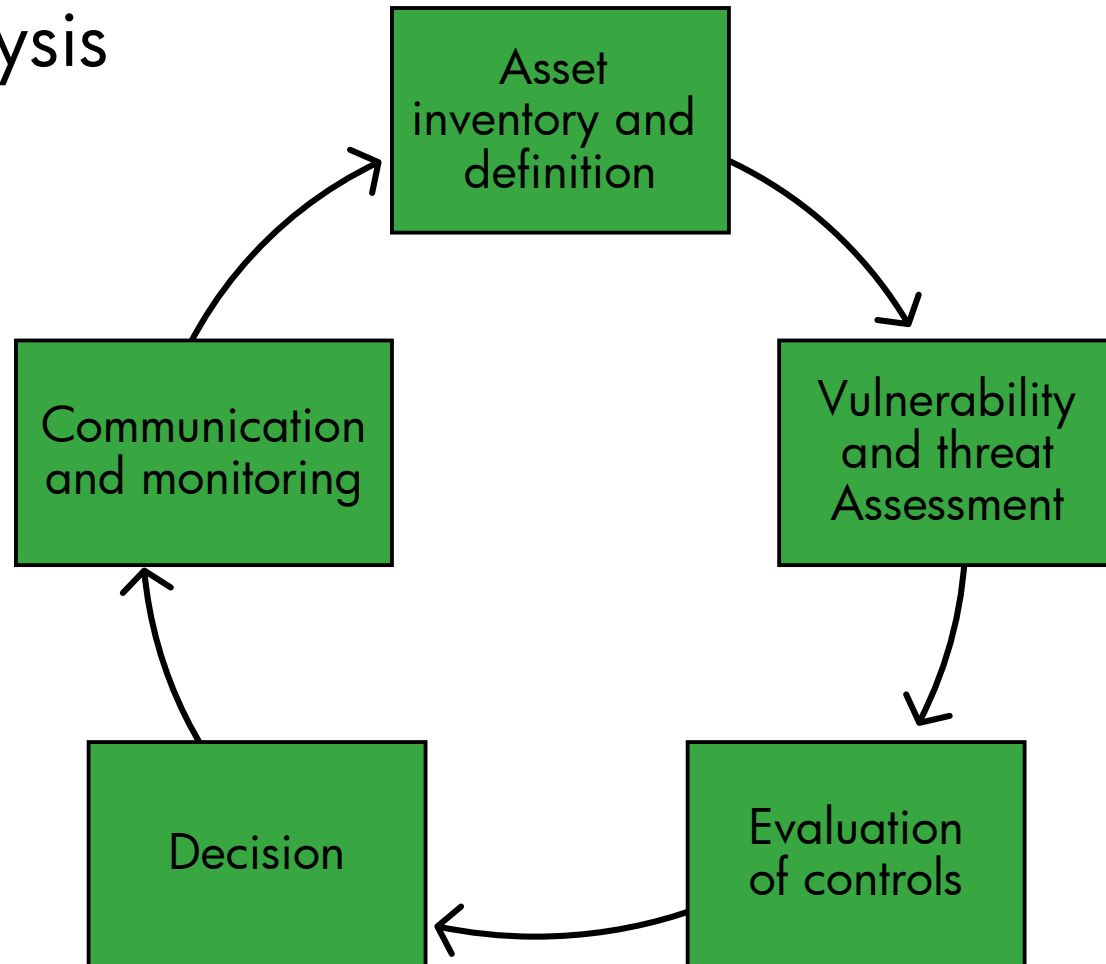


# Functional requirements phase

- Risk analysis and controls
- Business impact analysis
  - RTO
  - RPO
- Alternative strategies, cost benefit analysis, and budgeting

# Functional requirements phase

## Risk analysis



# Functional requirements phase

- Risk analysis
  - Quantitative—facts and figures, hard
    - Statistical
    - Actuarial
    - Annualized loss exposure (ALE)
    - Objective
  - Qualitative—not calculable, soft
    - Reputation
    - Future market share
    - Subjective



# Functional requirements phase

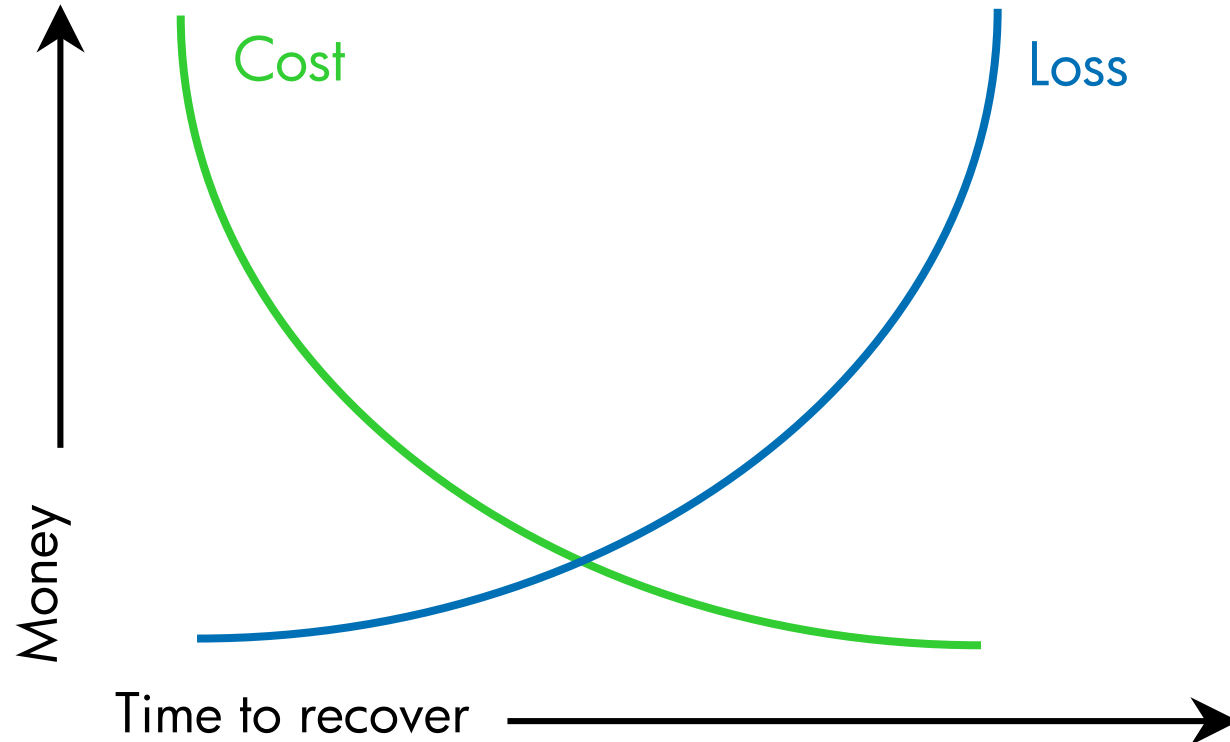
- Risk analysis
  - Annualized loss exposure (ALE)
    - Risk = frequency times exposure (to threat)
      - $R = f * E$  (E is exposure without control)
      - $r = f * e$  (e is exposure with control)
    - Benefit = exposure without control minus exposure with control minus the cost of maintaining the control
      - $B = R - r - c$
      - $B = f * (E - e) - c$

# Functional requirements phase

- Risk analysis
  - ALE does not cover
    - Time component of threat—5-minute loss versus 30-minute loss
    - Multiple controls for the same threat
    - Follow-on exposure, incidental damages
  - Controls do not reduce the threat—they reduce the exposure (and hence the risk)

# Functional requirements phase

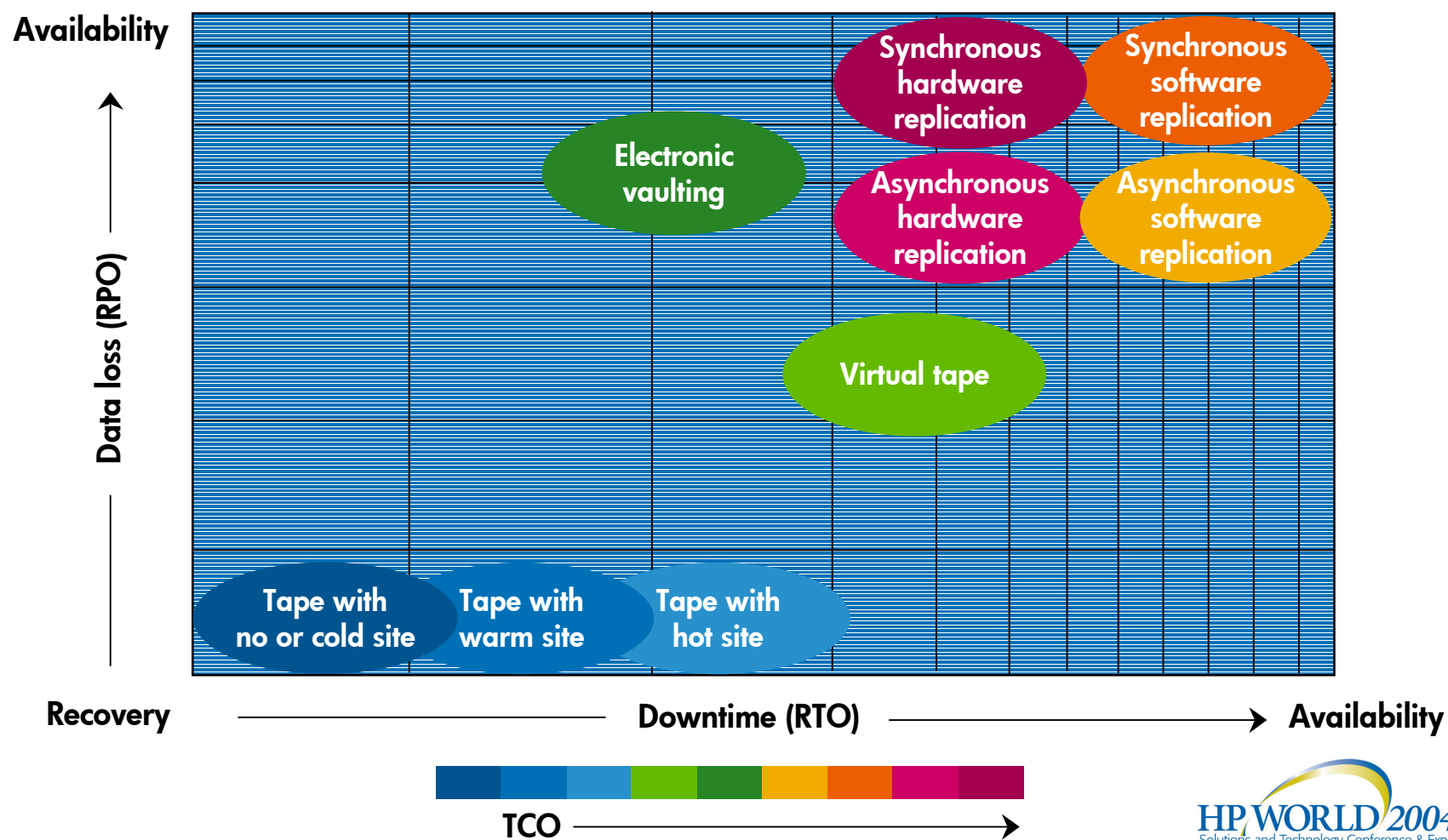
## Business impact analysis



# Functional requirements phase

- RTO
  - Recovery time objective
    - How soon after an event does the business process need to be available?
      - Not all business processes need to be available *at* the same time.
- RPO
  - Recovery point objective
    - How much work in progress can be lost?
      - Not all work needs to be recovered *to* the same time.

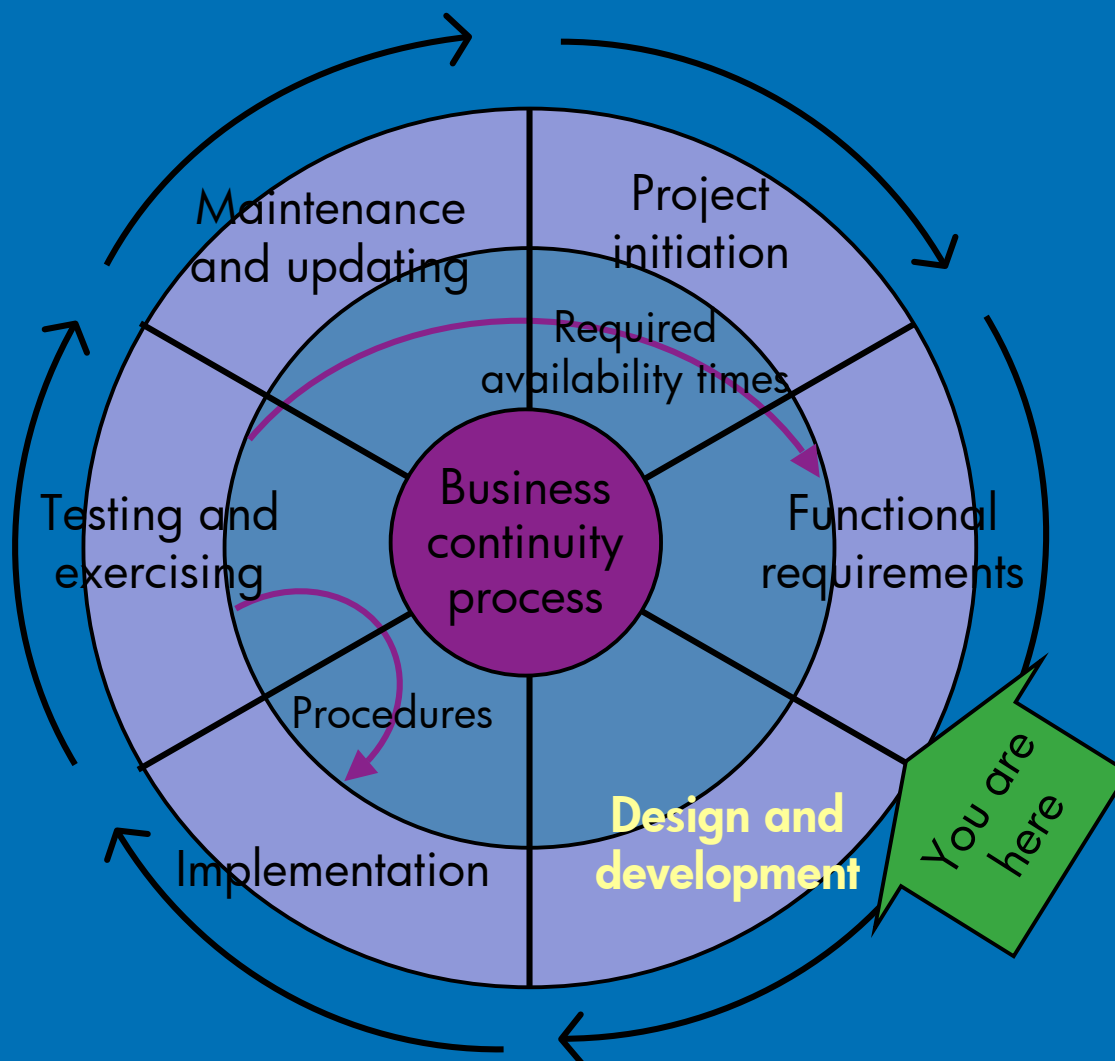
# It's a continuum



# Functional requirements phase

- Alternative strategies, cost benefit analysis, and budgeting
  - Does your plan make financial sense?





# Design and development phase

- Scope and objectives
- Deployment teams
- Cookbook
- Key disaster scenario
- Escalation, notification, and activation



# Design and development phase

- Scope and objectives
  - One department, one building, the campus, the entire company?
  - 100 percent of capacity or a subset?

# Design and development phase

- Deployment teams
  - Evaluation and declaration
  - Notification
  - Emergency response
  - Interim processing
  - Salvage
  - Relocation/reentry

# Design and development phase

- Cookbook
  - Common format for all plans
  - Step-by-step directions to write the plan
  - Corporate team description
  - Notification process
  - Plan considerations
  - Responsibility lists
  - Corporate team support forms

# Design and development phase

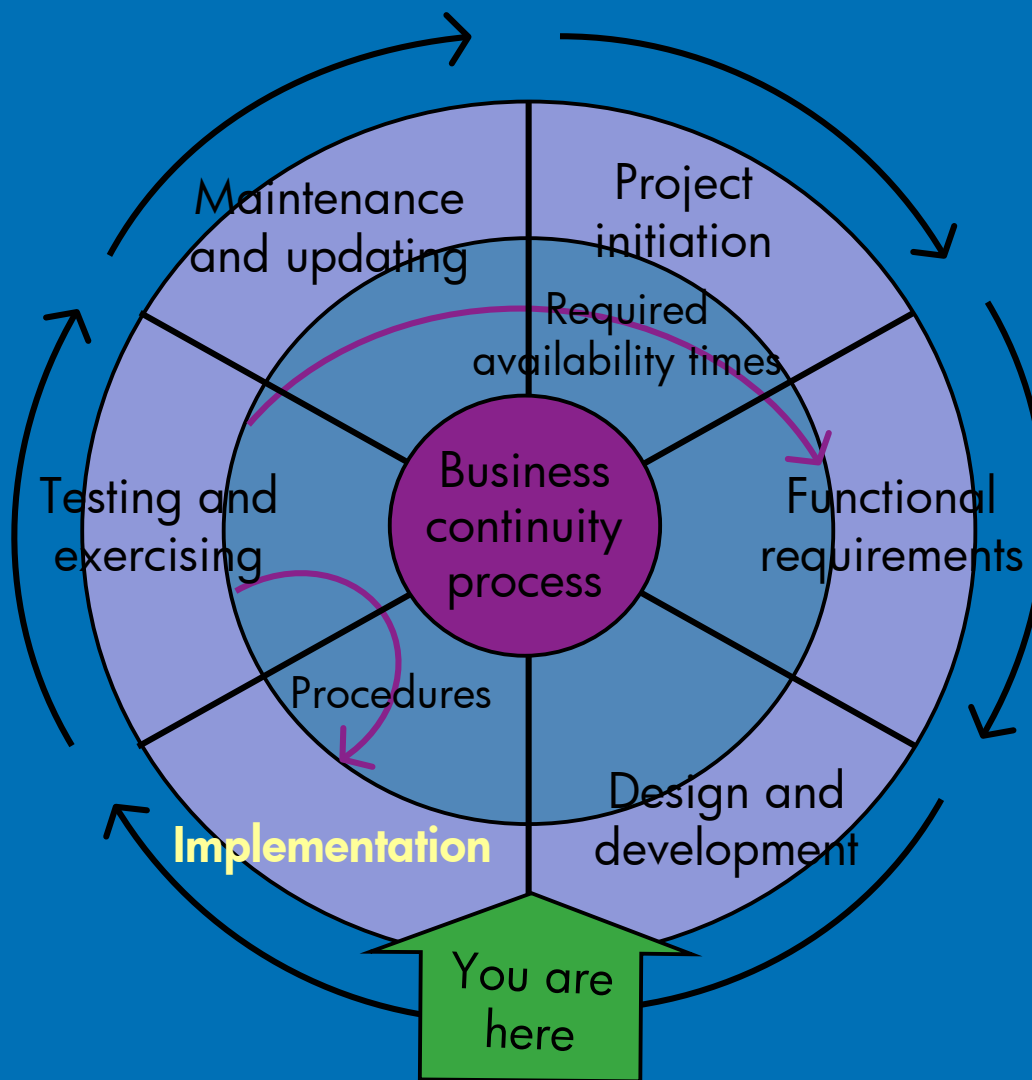
## Key disaster scenario:

“A fire broke out in the computer room. We are unsure of the state of the computers and data stored there. The building has been shut down by the fire department until they are sure that it is safe to enter. They are estimating that we will not have access to the building for a couple of days.”



# Design and development phase

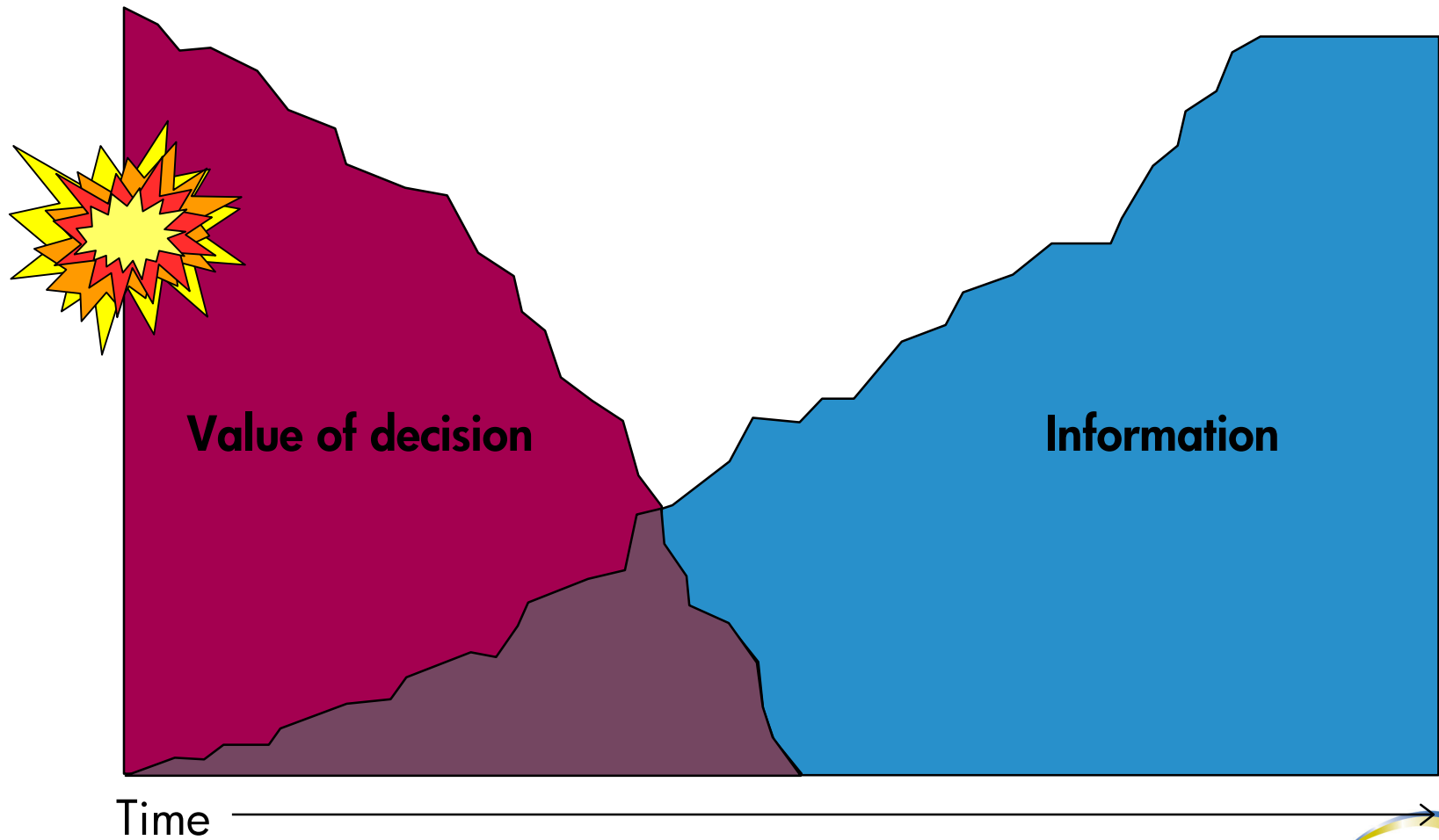
- Escalation, notification, and activation
  - Who activates the EMT?
  - How does the EMT get activated?
  - Who decides to activate the CMT?
  - How does the CMT get activated?
  - How does the CMT decide to activate the plan?
  - What happens if certain members of the CMT are unavailable?



# Implementation phase

- Emergency response
- Command and control
- Designation of authority
- Scripts
- Vendors and resources

# Implementation phase





# Implementation phase

- Emergency response
  - Evacuation, evaluation
    - Get your people somewhere safe—evacuation plans
    - When people are safe, evaluate the situation

# Implementation phase

- Command and control
  - Secure the area.
  - Gather information to make decisions.
  - Inform your employees.
  - Inform your stakeholders.
  - Inform the media.
  - Don't let the situation control you; if you need experts, hire them before you need them.

# Implementation phase

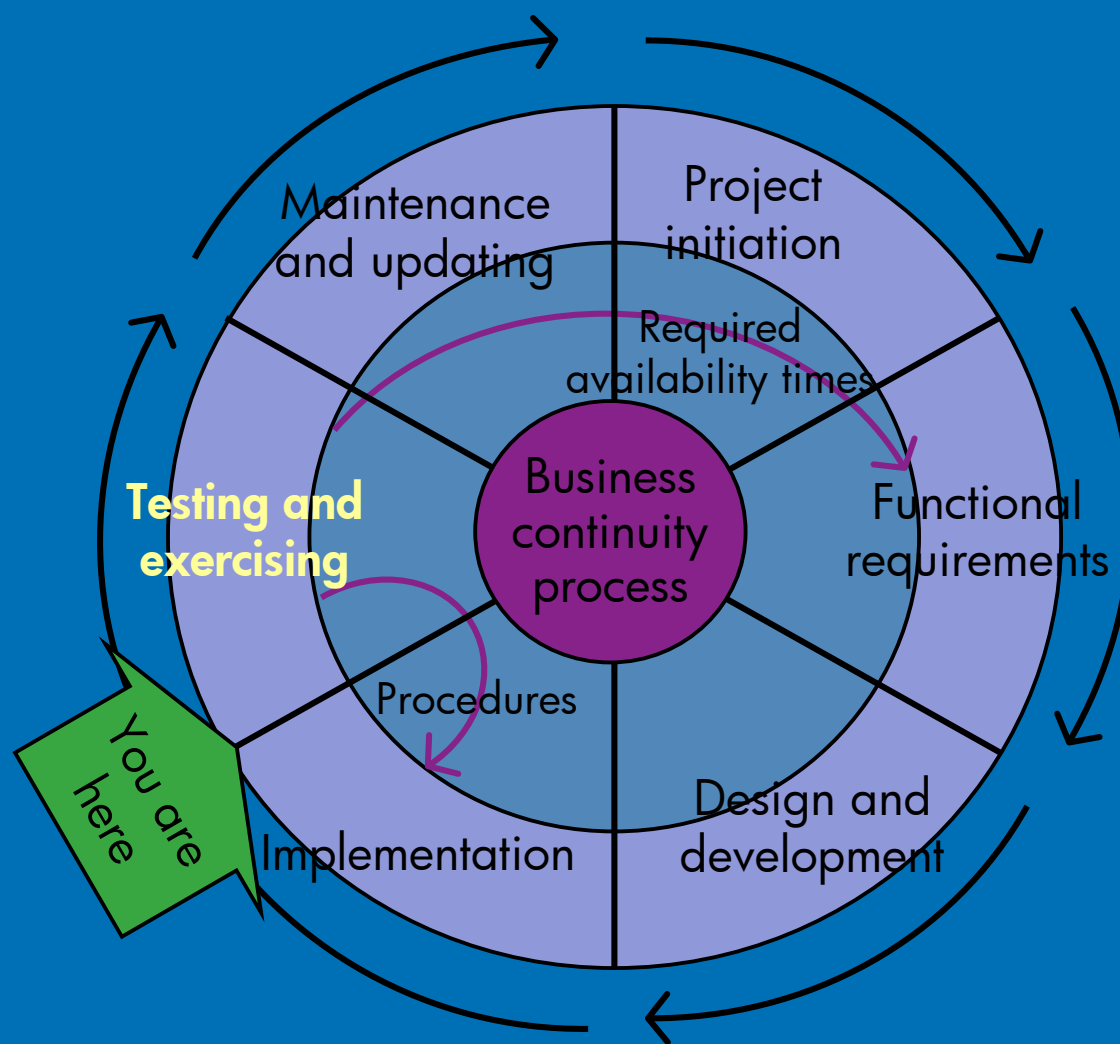
- Designation of authority
  - Who is in charge?
    - If they are not available, who is in charge?
      - If they are not available, who is in charge?
        - If they are not available, who is in charge?
  - Committees cannot be in charge.

# Implementation phase

- Scripts
  - Have a step-by-step listing of activities to be performed every step of the way.
    - In a disaster situation, people do not think rationally.
  - Scripts can be tested, tuned, and tested again.
    - The person who follows a script does not need to be the person who developed the script.
  - Automate as much as possible.
    - One customer has 800 automated scripts just for recovering the database.

# Implementation phase

- Vendors and resources
  - Hot site, warm site, cold site, off-site records storage
  - Equipment replacement
  - Rent-a-guard
  - Salvage experts
  - Catering
  - Hotel rooms, rental cars
  - Local authorities
    - Police, fire, hospitals, hazmat teams



# Testing and exercise phase

- Training and awareness
- Exercise program objectives, plans, and scenarios
- Evaluation and modification

# Testing and exercise phase

- Training and awareness
  - Employees need to know continuity planning concepts and terms.
  - It's a way of life that needs to be part of your everyday activities.
  - Your company (and therefore your job) is at stake.



# Testing and exercise phase

- Exercise program objectives
  - Practice makes perfect: some companies spend hundreds of hours tweaking parts of their plans to decrease recovery time.

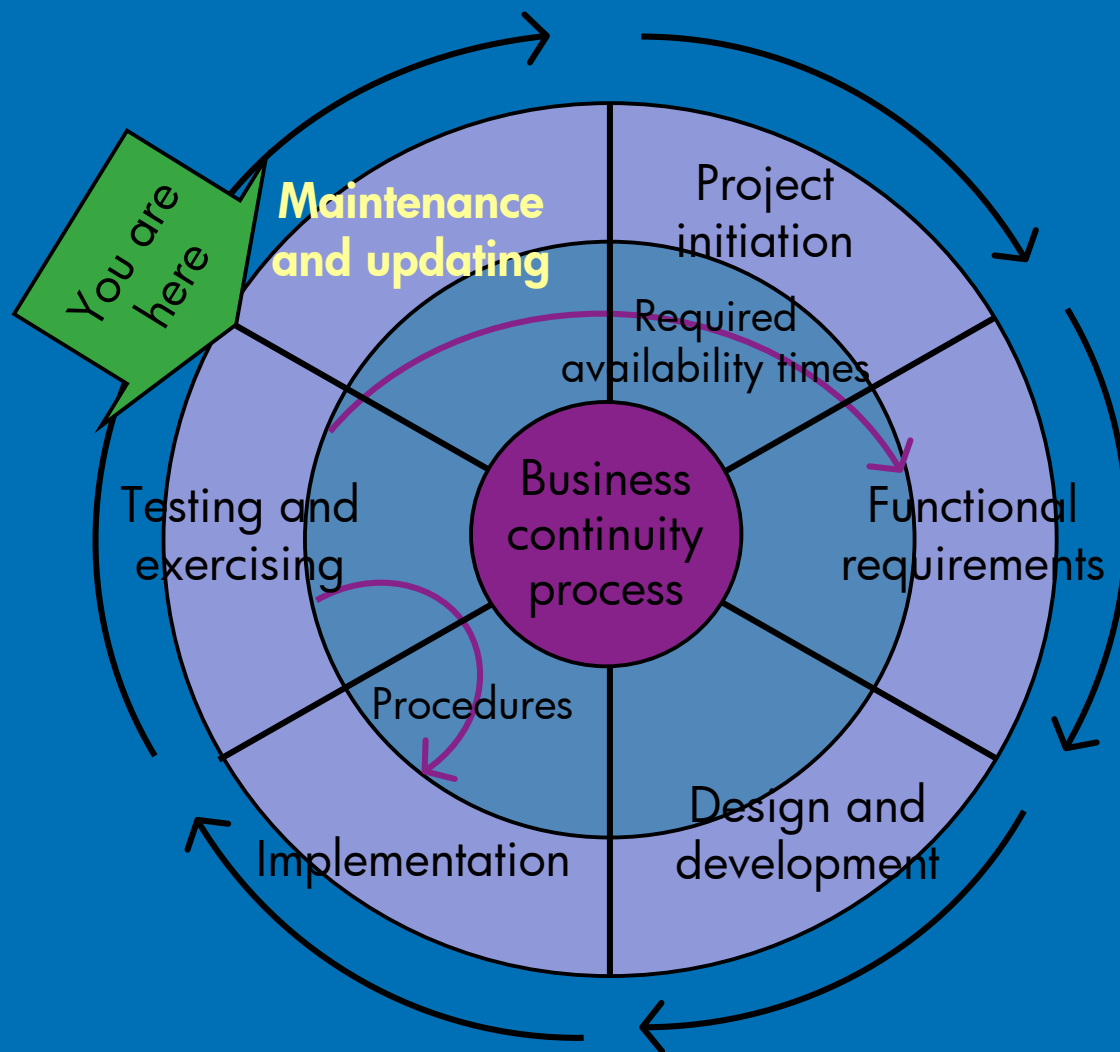
*Every second counts.*

# Testing and exercise phase

- Exercise plans and scenarios
  - How often, how much, how realistic?
  - Notify your people?
  - Notify the hot-site vendor?
  - Notify off-site storage?
  - Normal workday, middle of the night, or holiday weekend?

# Testing and exercise phase

- Evaluation and modification
  - What went wrong and how do we fix it for next time?
  - Do *not* find someone to blame; a fault found now could save your company later.
  - Were any of our assumptions wrong?
  - Do we need to revisit a previous phase?

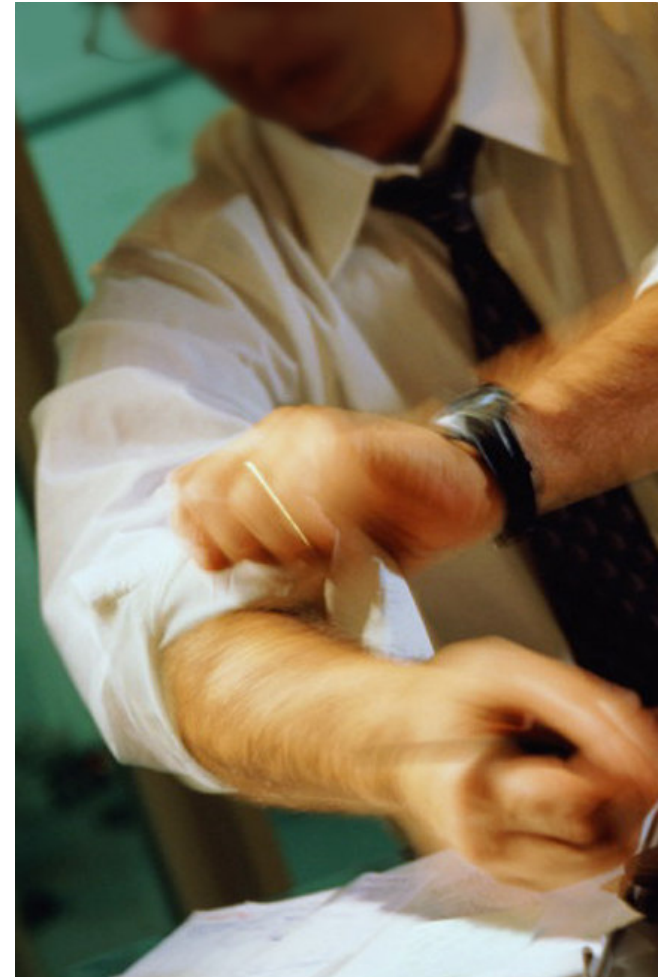


# Maintenance and update phase

- Remember to budget for this phase
  - An untested, stale plan is worse than no plan at all.
- Software tools?
- Review criteria
- Status, reporting, and audits
- Distribution and security
  - Your plan is a competitive asset.

# Execution phase

- If an event becomes a disaster
  - Decide
  - Declare
  - Notify
  - Execute



# Not just an IT problem

- IT can recover computers and applications, not business processes.
- The computers are humming, the applications are loaded ...

*... and no one is around to use them.*

Like Cheerios® are only part of a complete breakfast ...

*IT recovery is only part of a complete business continuity plan.*

# Horror stories





# Horror stories

- The backup site is in Atlantic city; declaration is during the Miss America pageant. (Hurricane Andrew)
- The computer room is in the basement, and there's a fire in the building. (Bell Canada)
- Will the generators be safe? Do you have a way to refuel them? (Tropical Storm Allison)

# Horror stories

- You power up the generators and nothing happens.
- You power up the generators and the power surge blows out your systems.
- You power up the generators and realize that your air conditioning isn't on backup power.

*Hint: exercise your plan*



# Food for thought



## Tapes

- Where is your tape backup hardware?
- Where are tapes stored until they go off-site?
- How quickly do your tapes go off-site?
- Are multiple tape copies sent via different routes?
- Do you do tape retrieval and restore tests?
- For recovery, do you ship tapes in "waves"?

# Food for thought



- The security code for pulling backup tapes from off-site storage is in your desk drawer.
- The phone number of your hot-site vendor is under a button in your auto dialer.
- What will you need that's stored in your Rolodex?
  - (Some people never learn.)

# Food for thought

- Replicated enterprise storage
  - Vendors guarantee disk integrity.
    - Backup disk = primary disk at a bit level
  - Transactional integrity is *not* guaranteed.
  - Your OS needs to recover the crashed disk
  - Your database software needs to recover the database to a consistent state before you can begin processing on the backup system.





# Food for thought

- You updated your application and changed the database format.
- Software replication will not work unless you change the database format on your backup system, but did you remember to copy over the new object files?



# Food for thought



- Check your third-party site contract.
  - How many other companies in the same threat area use the same vendor?
  - How soon do you have to vacate? Where will you go?
  - Have you included workstations and allocated space for them?

# Remember that building?

To this day, the tornado-scarred Bank One tower in Fort Worth, Texas, is still closed.



30 March 2000



10 February 2001



# And finally ...

- 43% percent of the businesses in the New York World Trade Center were out of business within a year of the 1993 bombing.
- 70% of the businesses that were in the towers, 90% of the businesses that were in the complex, as well as 162,000 jobs that existed on the morning of 9/11/2003, vanished by mid 2003.



# For more information...

- **Useful URLs**
  - <http://www.hp.com/go/continuity>
  - <http://www.hp.com/go/nonstopcontinuity>
- **Product manager for continuity products**
  - [ron.lapedis@hp.com](mailto:ron.lapedis@hp.com)

# HP WORLD 2004

Solutions and Technology Conference & Expo

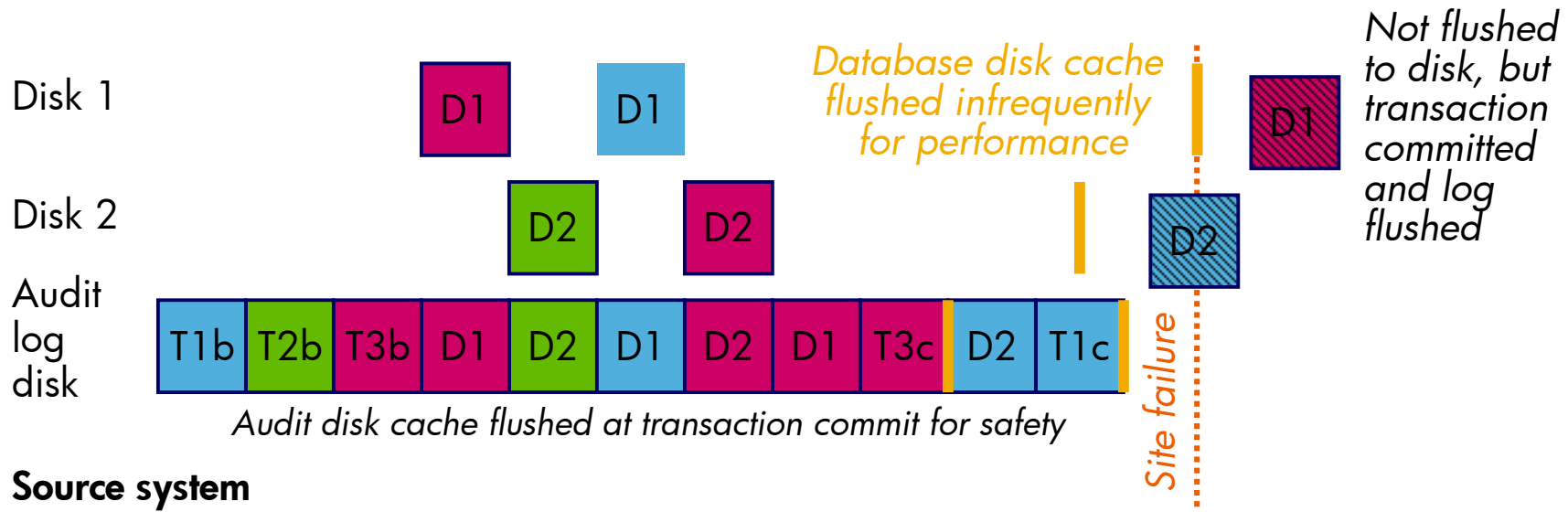
Co-produced by:



RECOMMENDED TRAINING VENUE FOR THE  
**HP Certified Professional**

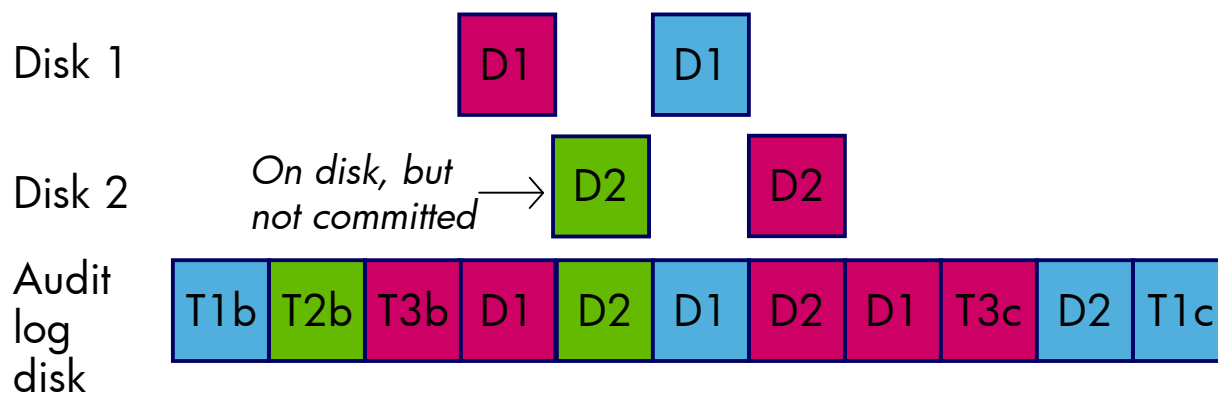



# Physical disk does not equal logical database



## Source system

## Target system



 = Disk cache flush