



Best practices: Application uptime is no accident

Ron LaPedis

CBCP, CISSP, ISSAP, ISSMP

June 2005



Agenda

Information security
Business continuity
What HP has to offer





Information security

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

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 are not
- Authentication—who you are
- Authorization—what are you allowed to access?
- Privacy—should you be allowed in the first place?



Identification, authentication, authorization, and privacy



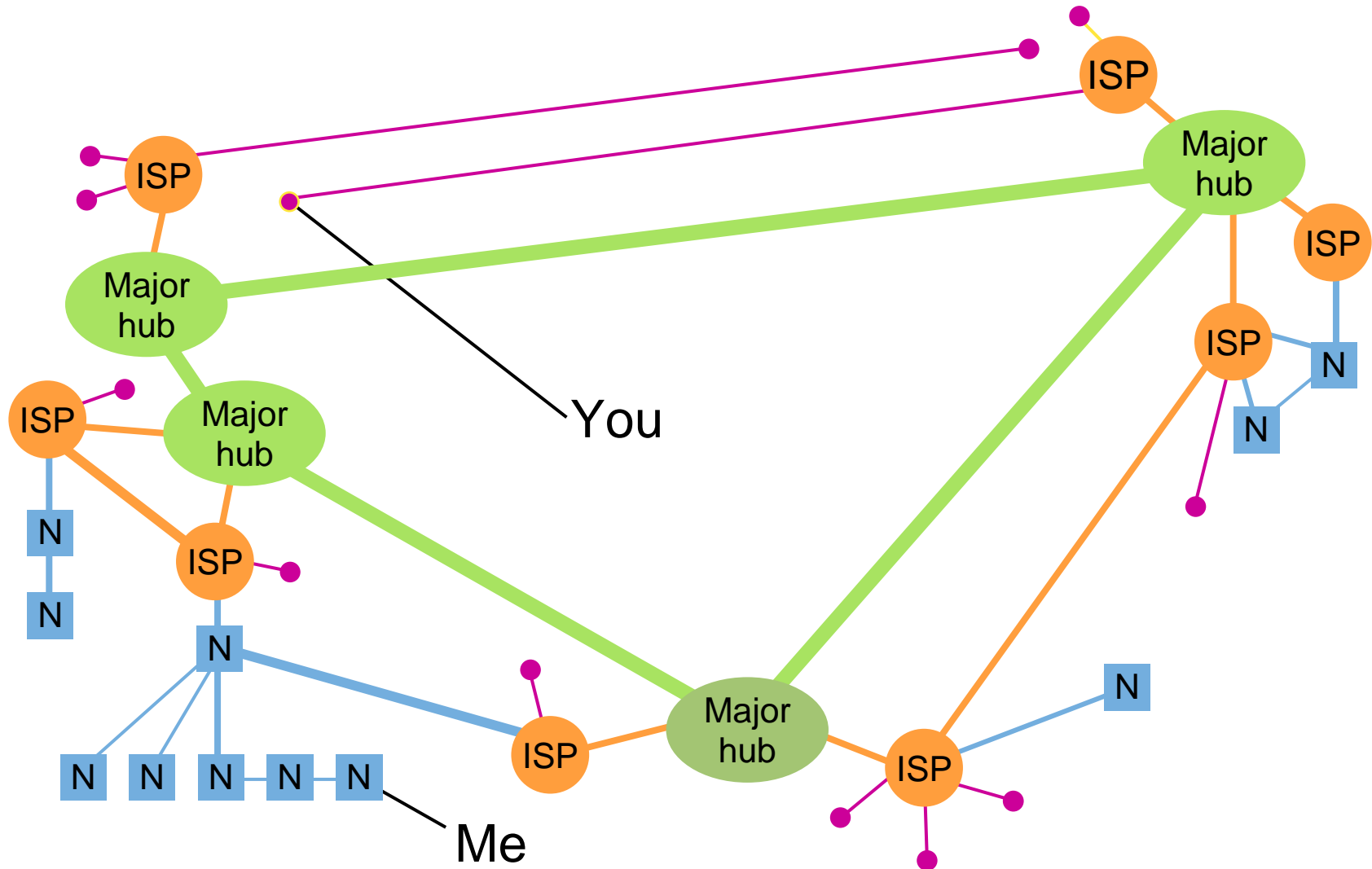
- Proper user verification
- What business information goes online and who can access it?
- Interception of business information
- Hacking of business information
 - Extortion
 - Liability

- 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

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

- Must flow from corporate policy
- Should be stated on your web site
- 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
- Phishing
 - <http://www.identityprotection101.com/phishing>
- Classification of business information and least privilege

What does the Internet look like?

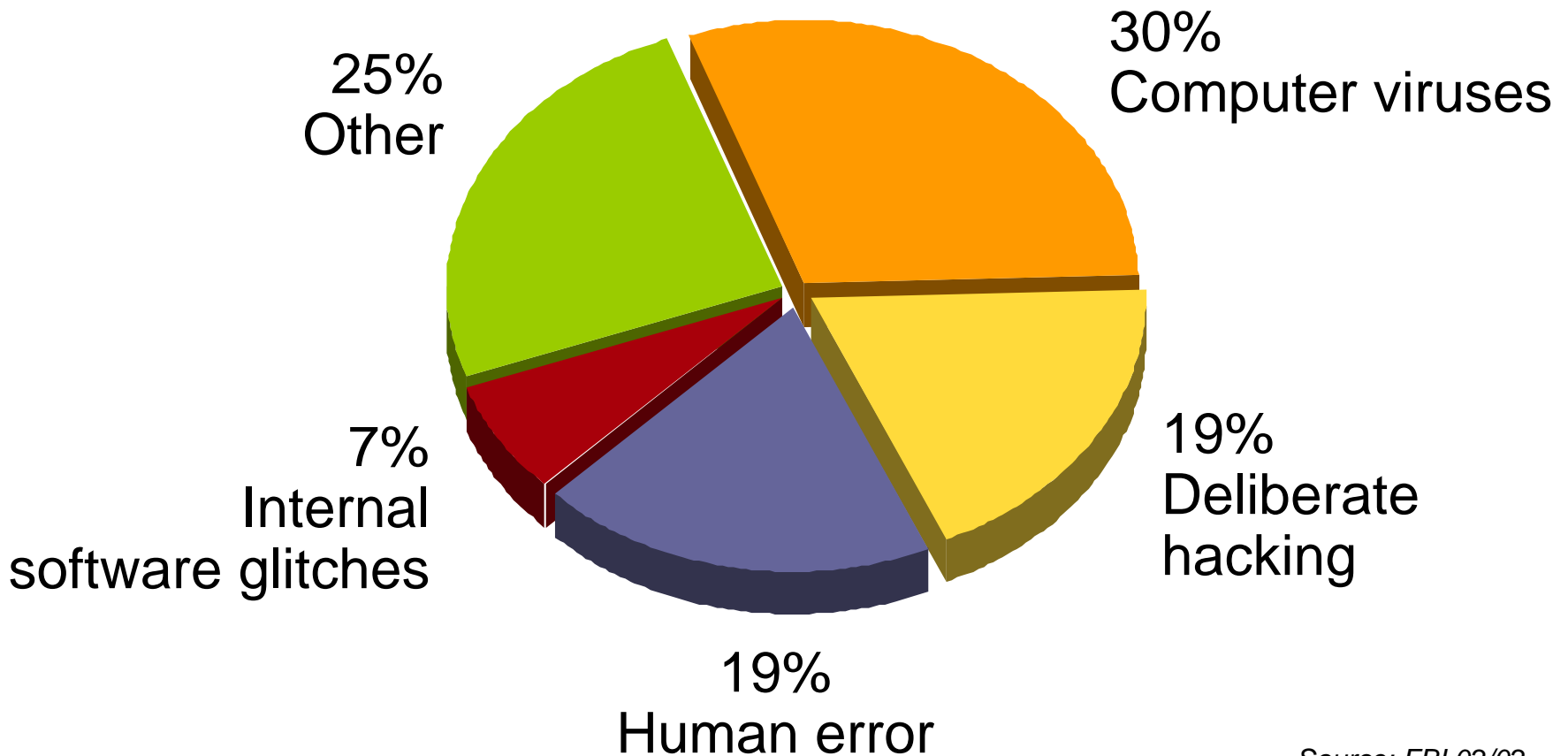


Where do hackers come from?

- Most information security breaches come from insiders.
- Companies usually keep quiet about breaches.



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 communications
- Encrypted databases, if necessary
- Multi-tier architecture
- Hardware key management

Where do I start?



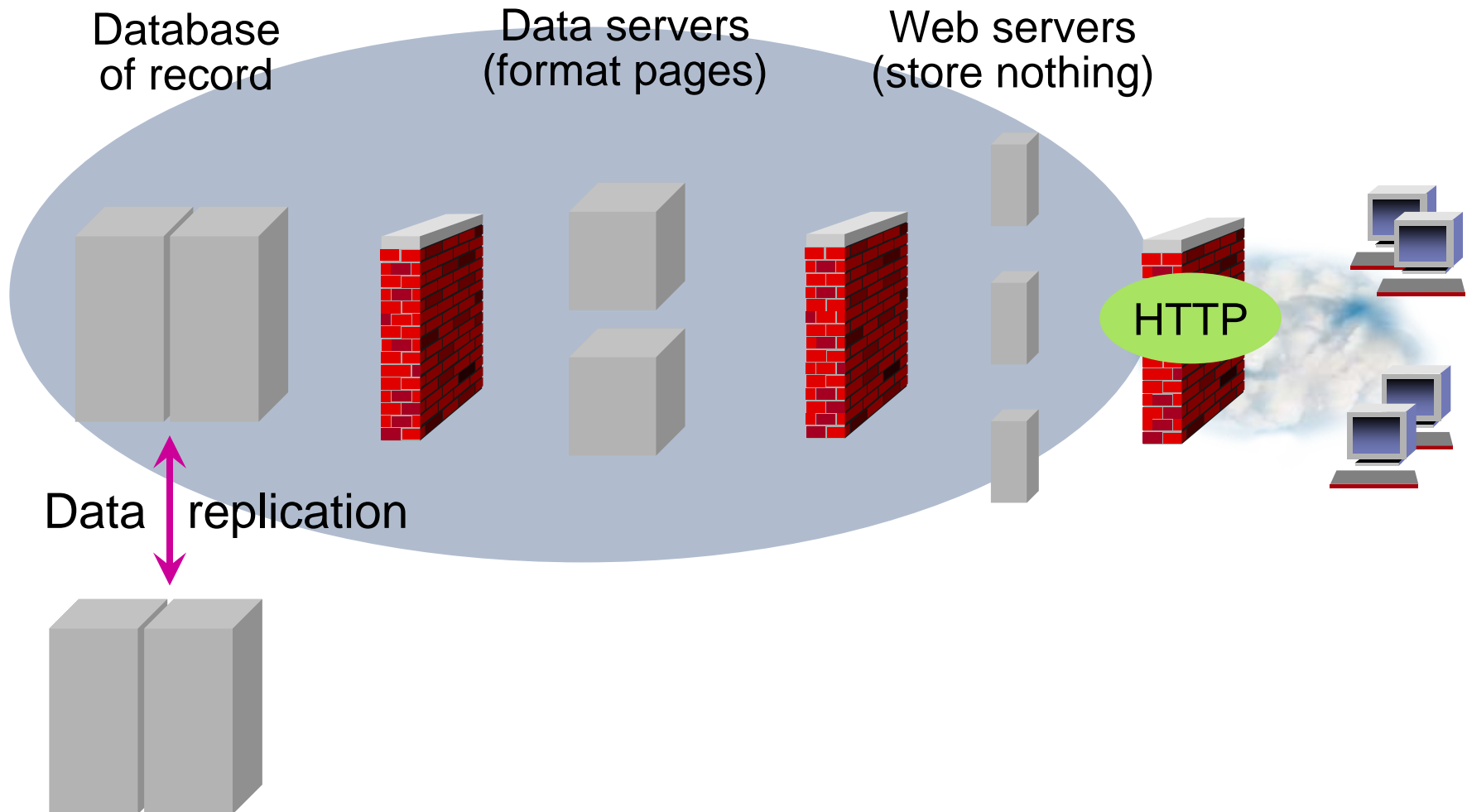
- Don't store anything on Web servers because they can be hacked.
- Subscribe to patch lists like bugtraq.
 - www.securityfocus.com
- Carefully evaluate the hardware and software you are using for inherent security.

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



- Don't tempt even loyal employees.
 - 82 percent of bank computer fraud committed by insiders (Ernst and Young, 2000).
- 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.

- 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



- 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.

Top 10 Vulnerabilities to Windows Systems



- W1 Web Servers & Services
- W2 Workstation Service
- W3 Windows Remote Access Services
- W4 Microsoft SQL Server (MSSQL)
- W5 Windows Authentication
- W6 Web Browsers
- W7 File-Sharing Applications
- W8 LSAS Exposures
- W9 Mail Client
- W10 Instant Messaging

Top 10 Vulnerabilities to UNIX Systems



- U1 BIND Domain Name System
- U2 Web Server
- U3 Authentication
- U4 Version Control Systems
- U5 Mail Transport Service
- U6 Simple Network Management Protocol (SNMP)
- U7 Open Secure Sockets Layer (SSL)
- U8 Misconfiguration of Enterprise Services NIS/NFS
- U9 Databases
- U10 Kernel

Why HP Integrity 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.

- HP has a simple product strategy: to build security into our products, include interfaces for partners to extend and enhance the native security of HP Integrity NonStop servers, and tie everything together with HP Services.

Security partners



- Baker Street Software www.bakerstreetsoftware.com
- Bowden Systems www.bsi2.com
- BrightStrand International www.brightstrand.com
- CA (Computer Associates) www.ca.com
- CAIL www.cail.com
- comForte www.comforte.com
- Cross-EL www.crossel.com
- Crystal Point www.crystalpoint.com

Security partners



- CSP (Computer Security Products) www.cspsecurity.com
- GreenHouse www.greenhouse.de
- Gresham Software Labs www.greshamsoftwarelabs.com
- K2Defender www.k2defender.com
- Insession Technologies www.insession.com
- Nexsion, Inc www.nexsion.com
- Unlimited Software Assoc. www.usahero.com
- XYPRO www.xypro.com

Security partner product features



- Access control list (ACL) management, Guardian
 - Baker Street, CSP, GreenHouse, XYPRO, Cross-EL
- ACL management, OSS
 - Baker Street
- Audit reports, Guardian
 - Baker Street, CA, CAIL, CSP, GreenHouse, Gresham, Insession, XYPRO, Cross-EI
- Audit reports, OSS
 - Baker Street, CAIL, CSP, GreenHouse, Insession, XYPRO, Cross-EI
- Audit reports, consolidated
 - Baker Street, CSP, GreenHouse, Insession, XYPRO

Security partner product features



- Authentication, location-based
 - Bowden , BrightStrand, comForte, Cross-EI, CSP, GreenHouse, Insession Intl., XYPRO
- Authentication, multi-factor
 - CA, comForte, Cross-EI, CSP, GreenHouse, Insession, XYPRO
- Authentication, time-based
 - Bowden, CA, comForte, Cross-EI, CSP, GreenHouse, XYPRO
- Authorization, command-level: Guardian
 - Bowden, CA, Cross-EI, CSP, GreenHouse, Gresham, XYPRO
- Authorization, command-level: OSS

Security partner product features



- CMON process
 - BrightStrand, XYPRO
- Encryption toolkit, SSH for OSS
 - Bowden, CAIL, comForte, Crystal Point, CSP
- Encryption toolkit, SSH for Guardian
 - Bowden, CAIL, comForte, Crystal Point
- Encryption toolkit, SSL for OSS
 - Bowden, CAIL, comForte, Crystal Point, Gresham, Insession, Nexsion, XYPRO
- Encryption toolkit, SSL for Guardian
 - Bowden, CAIL, comForte, Crystal Point, Gresham, Insession, Nexsion, XYPRO

Security partner product features



- Encryption, file transfer (SSH)
 - Bowden, CAIL, comForte, Cross-EI, Crystal Point, CSP, Gresham, Insession
- Encryption, file transfer (SSL)
 - Bowden, CAIL, comForte, Cross-EI, Crystal Point, CSP, Gresham, Insession, XYPRO
- Encryption, Guardian terminal sessions
 - Bowden, BrightStrand, CAIL, comForte, Crystal Point, CSP, Gresham, Insession, XYPRO, Cross-EI
- Encryption, OSS terminal sessions
 - Bowden, CAIL, comForte, Crystal Point, CSP, Insession, XYPRO, Cross-EI
- Encryption, password over LAN
 - Bowden, CA, CAIL, comForte, Crystal Point, CSP, Greenhouse, Gresham, Insession, XYPRO, Cross-EI

Security partner product features



- Encryption, database (record or field level)
 - GreenHouse, Insession, XYPRO
- Encryption, whole file
 - Bowden, Cross-EI, CSP, GreenHouse, XYPRO
- Encryption, hardware module support
 - Greenhouse
- Encryption, key management
 - Greenhouse, Insession, XYPRO
- Encryption, certificate generation & management
 - Crystal Point
- GUI for security administration
 - Baker Street, CA, CAIL, Cross-EL, CSP, GreenHouse, Gresham, XYPRO
- Intrusion detection system
 - Baker Street, CA, CSP, GreenHouse, XYPRO, K2Defender, Cross-EI

Security partner product features

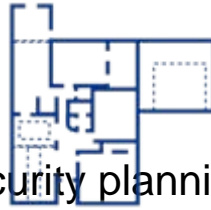


- Keystroke logging, Guardian
 - CAIL, comForte, Cross-EL, Crystal Point, CSP, GreenHouse, XYPRO
- Keystroke logging, OSS
 - CAIL, comForte, Cross-EL, Crystal Point, CSP, GreenHouse, XYPRO
- Password management, multiple systems
 - CA, Cross-EL, CSP, GreenHouse, Gresham, XYPRO
- Password quality
 - Bowden, CA, Cross-EL, CSP, GreenHouse, XYPRO
- Password reset, delegated
 - CA, Cross-EL, CSP, GreenHouse, XYPRO
- Policy management, enforcement
 - Bowden, CA, Cross-EL, CSP, GreenHouse, Gresham, XYPRO
- Single Sign-On (SSO)
 - Bowden, CA, Cross-EL, GreenHouse, Gresham, Insession, XYPRO



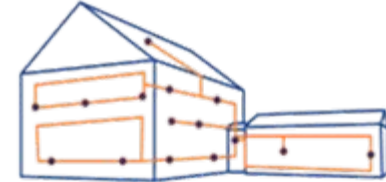
Business and commerce enabling security

- Fraud Management
- Secure Internet Banking
- Secure Payment
- E-Commerce Back Office Solutions
- Securing Mobile Services Delivery Platform



Security planning and governance

- Risk, Threat and Vulnerability Assessment
- Security Strategy and Policy Services
- Security Training and Awareness



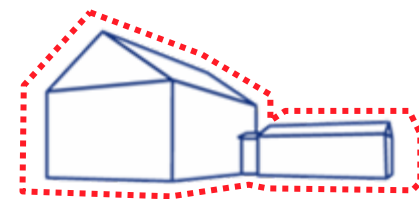
Trustworthy infrastructure

- Physical Asset Protection
- System and Host Security
- Network Security
- Secure E-mail
- Secure Printing
- Application Scanning



Identity and access management

- Identity Provisioning
- Access Management
- Directory Integration



Security management

- Security Event Correlation
- Security Incident Management
- Patch Management
- Managed Security

Introduction to continuity planning

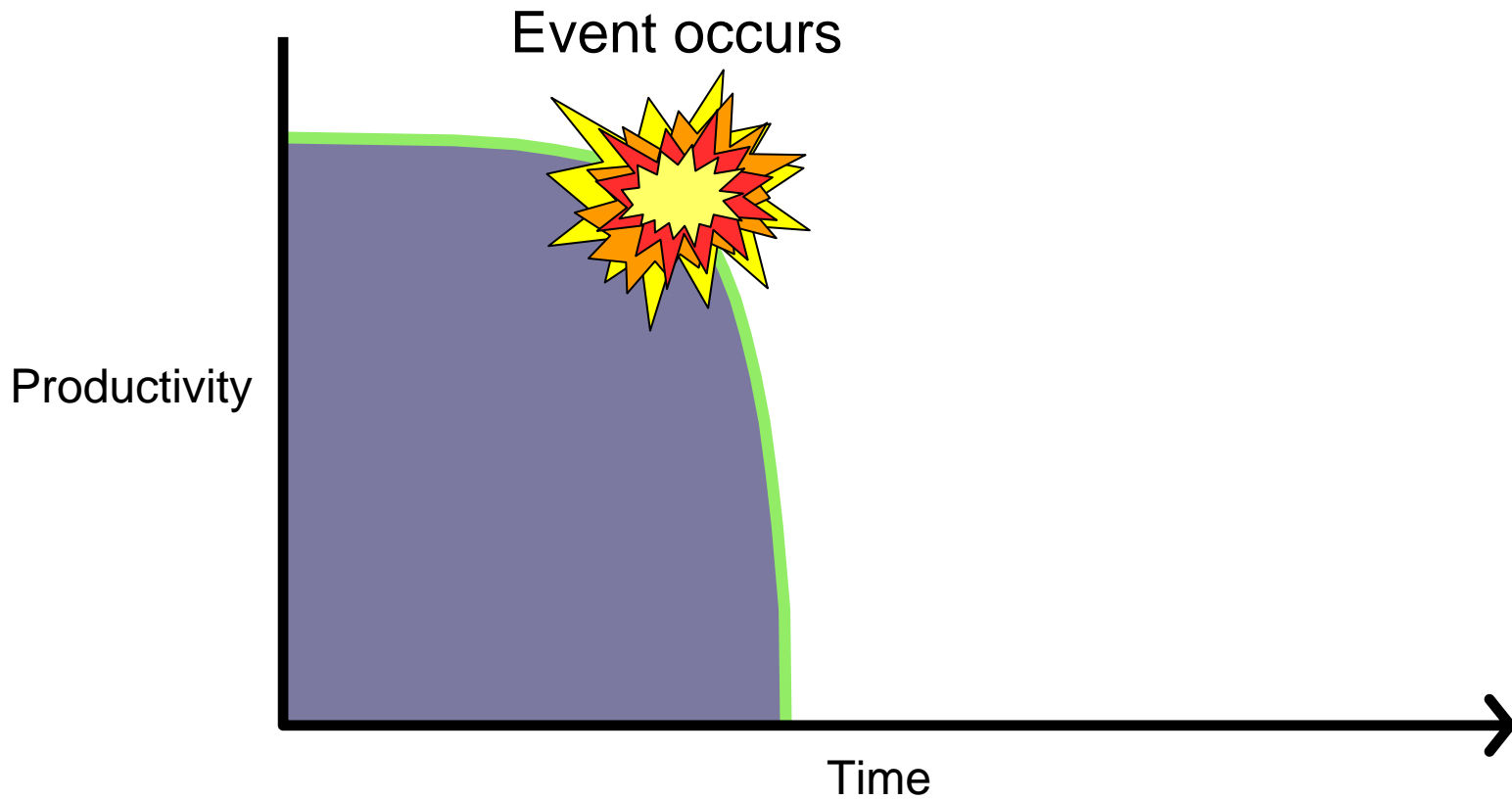


Agenda

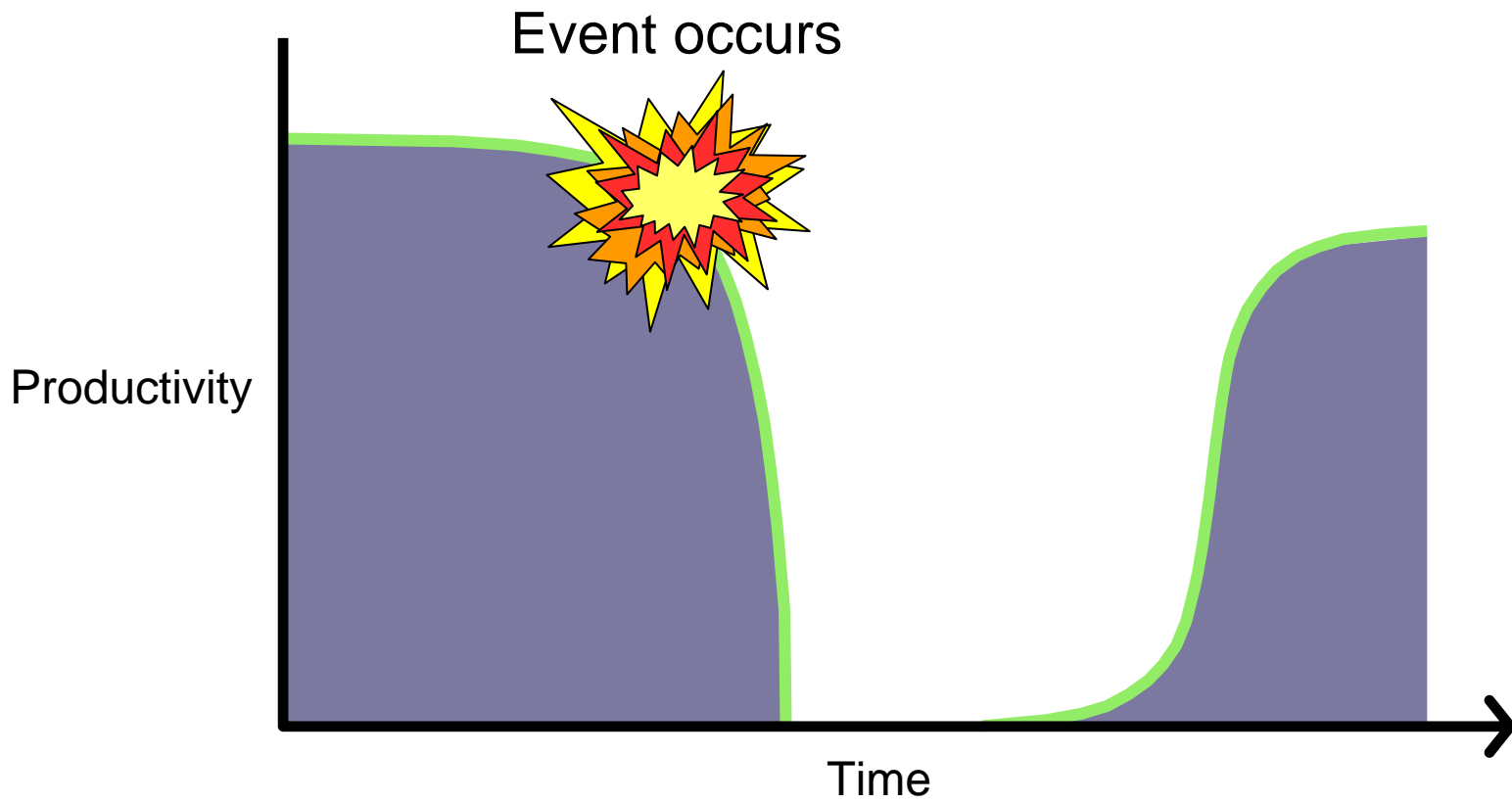
- Continuity planning? I thought it was called disaster recovery.
- Why?
- Professional practices
- Continuity planning activities
- Step by step
- Horror stories
- Food for thought



Something happens

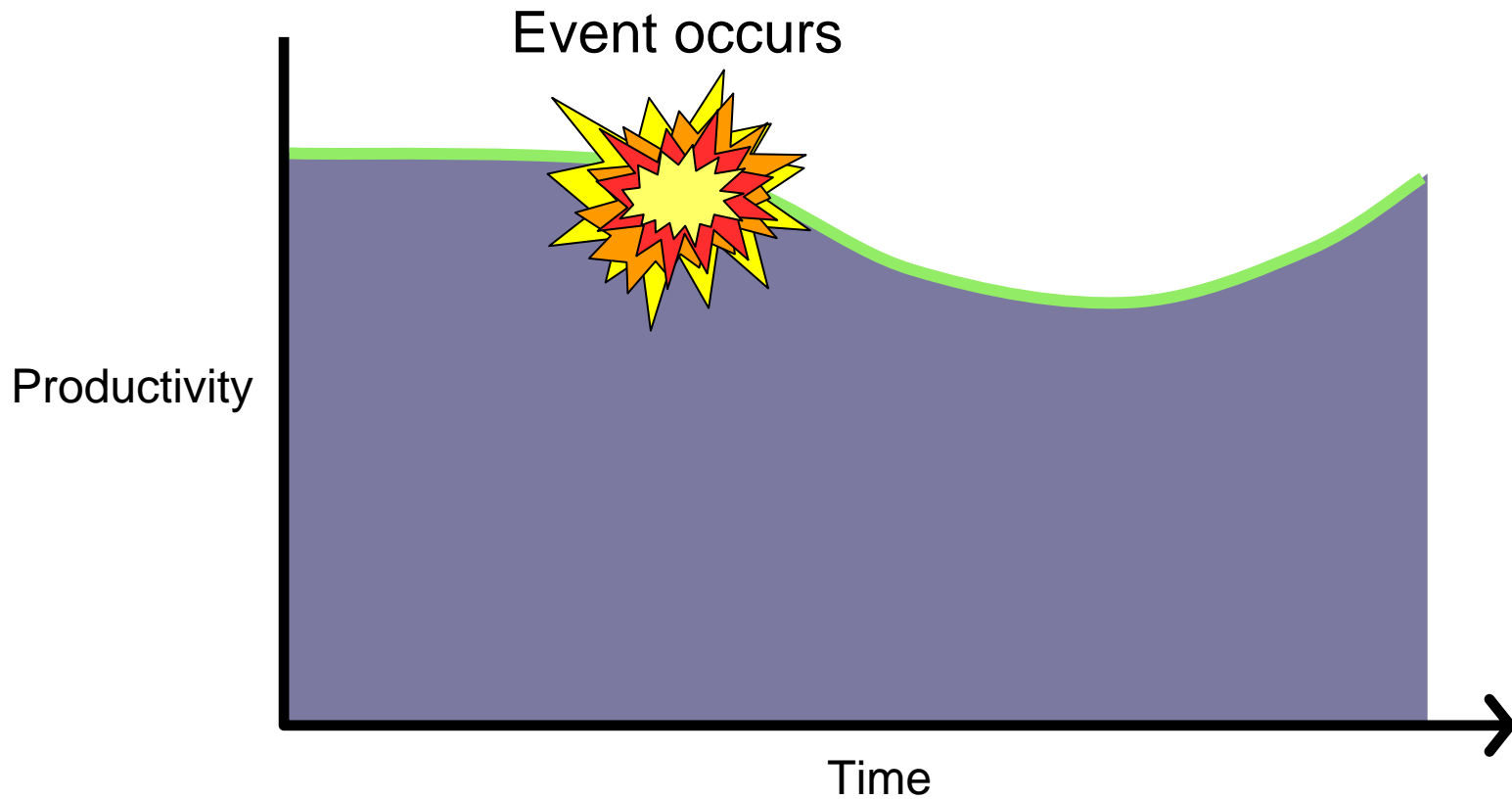


Disaster recovery



Source: DRII

Business continuity



Source: DRII

Why?



Downtime is not acceptable



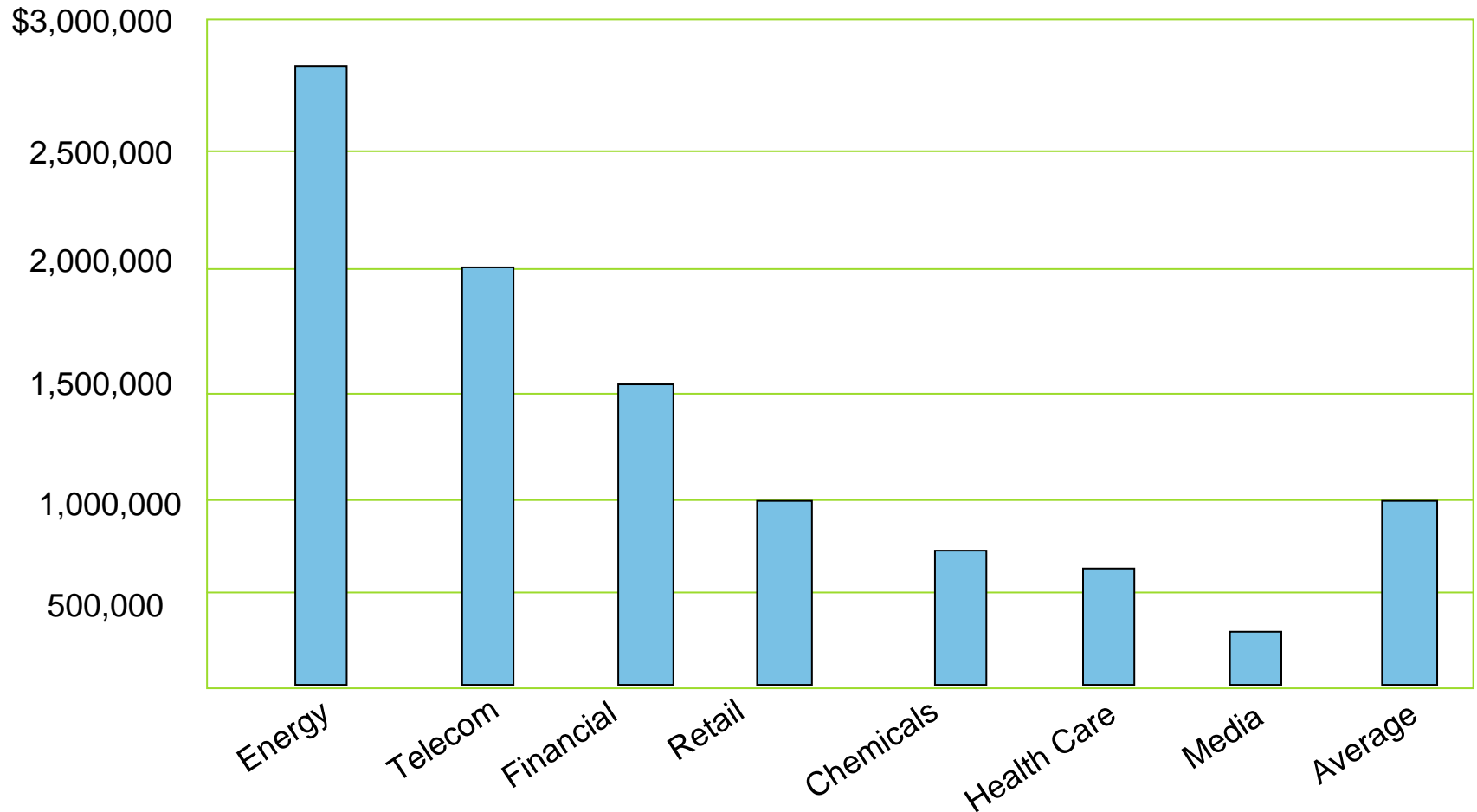
- Time zones are no longer a barrier to conducting business.
- If your site is down, your competition is one click away.
 - Utility failure
 - Communications failure
 - System failure
 - Application failure
 - Operating system failure
 - Utility upgrade
 - Communications upgrade
 - System upgrade
 -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

And what about
system and database
maintenance?

Business impact of downtime is high

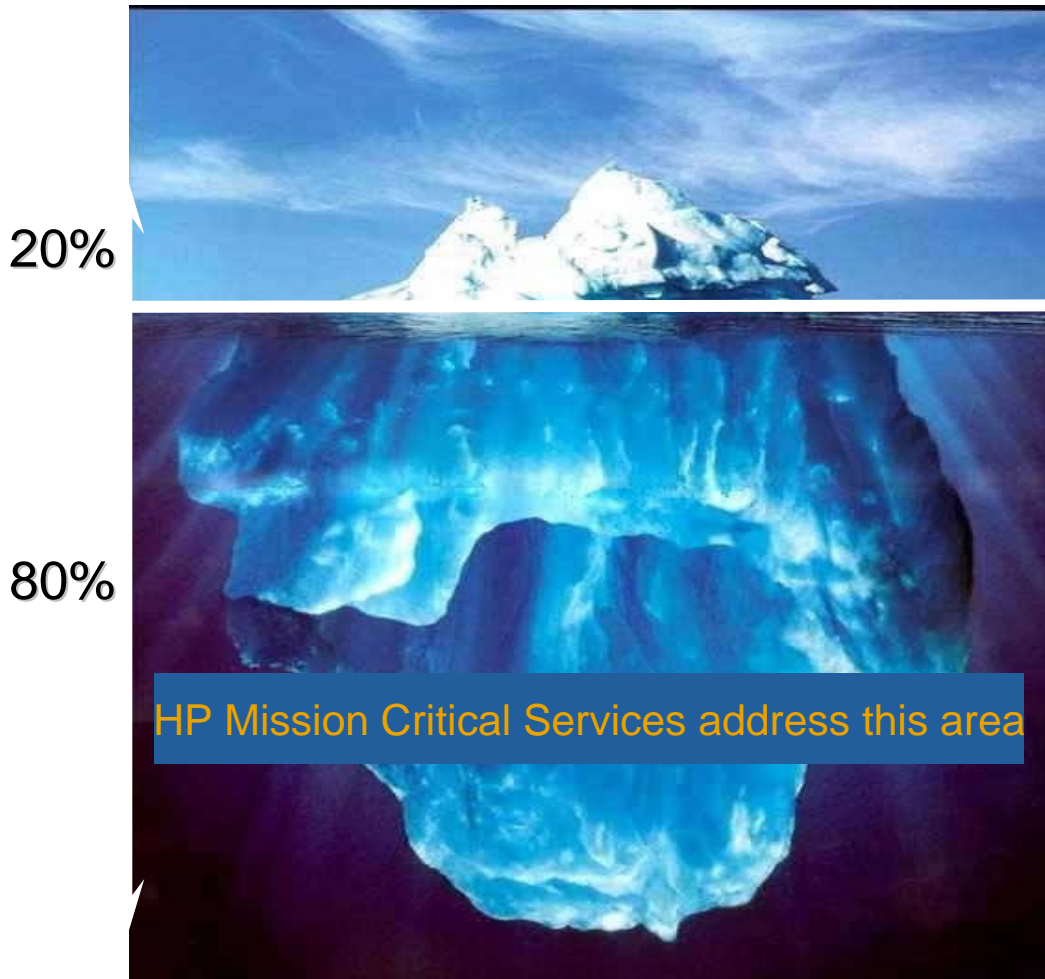


Cost per hour



Source: Contingency Planning and Management, May/June 2003

Causes of downtime



Technology:
Hardware failures

Processes and people:
Software(20%) and network(15%) issues, human error(10%), security breaches(5%) , unknown causes (30%)

“80% of unplanned downtime is due to people and processes.”

-Source: Gartner

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

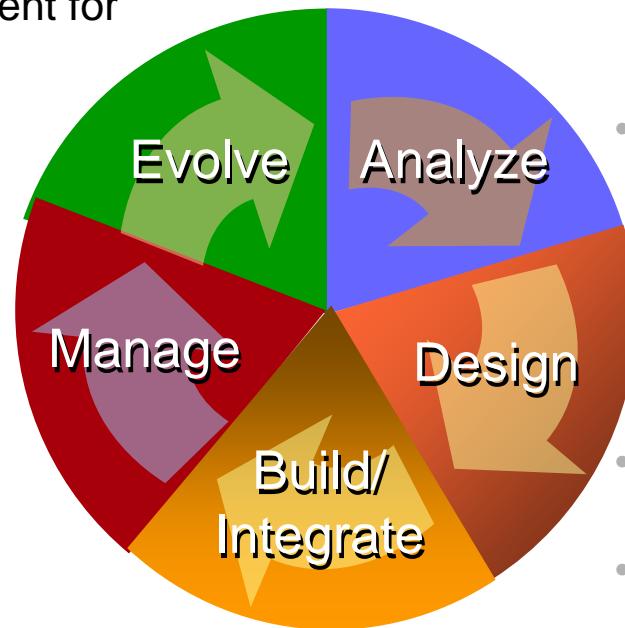


- Ensures that an event doesn't become a *disaster*
- Covers a broad spectrum of business and technology issues
- The key goal: required business process availability

HP's Business Continuity & Availability methodology



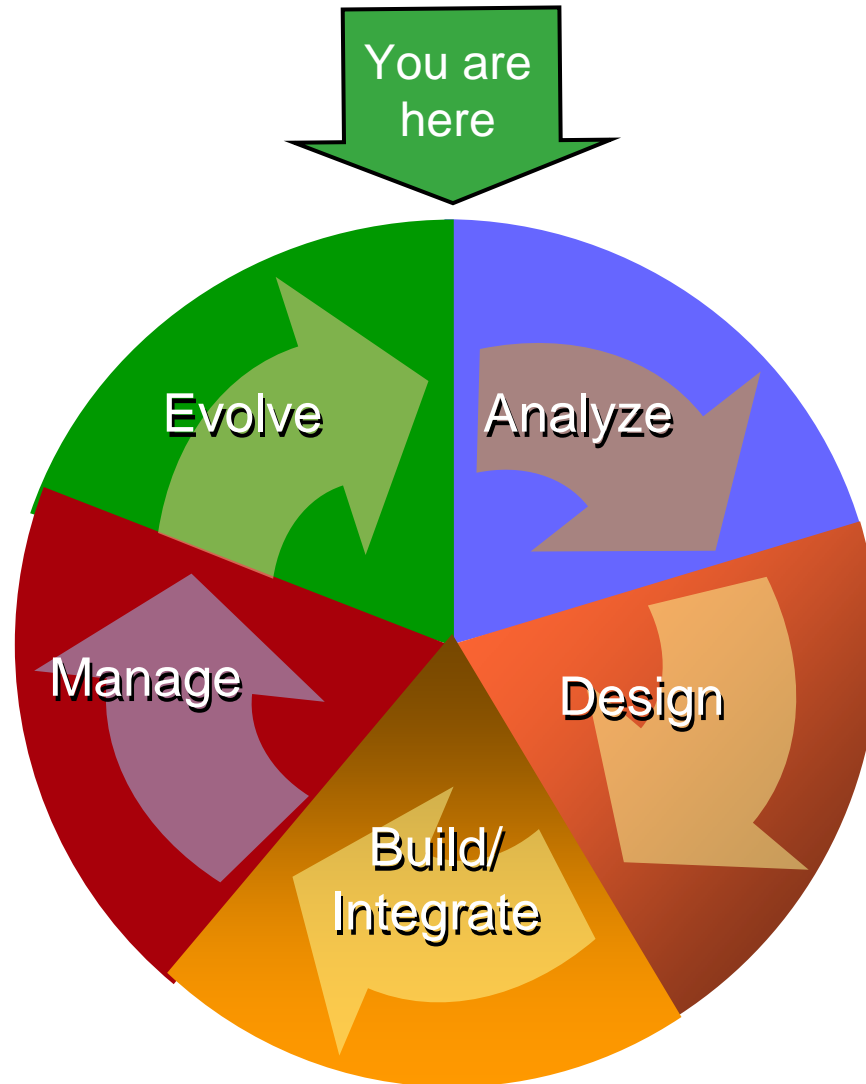
- Integrate into change management process
- Audit/assess environment for improvements
- Service level reporting and analysis
- Ongoing monitoring, measurement, and management
- Automation of IT processes
- Test/rehearse BC&A plan regularly



- Identify & mitigate business and operational risks.
- Quantify cost of outage of key business processes (direct & indirect)
- Define availability and objectives for each business process
- Evaluate strategy & technology alternatives
- Architect solution to meet objectives (including detailed design of infrastructure and processes)

- Develop overall BC&A plan to ensure continuity for the business
- Implement and integrate infrastructure and processes.
- Train staff.

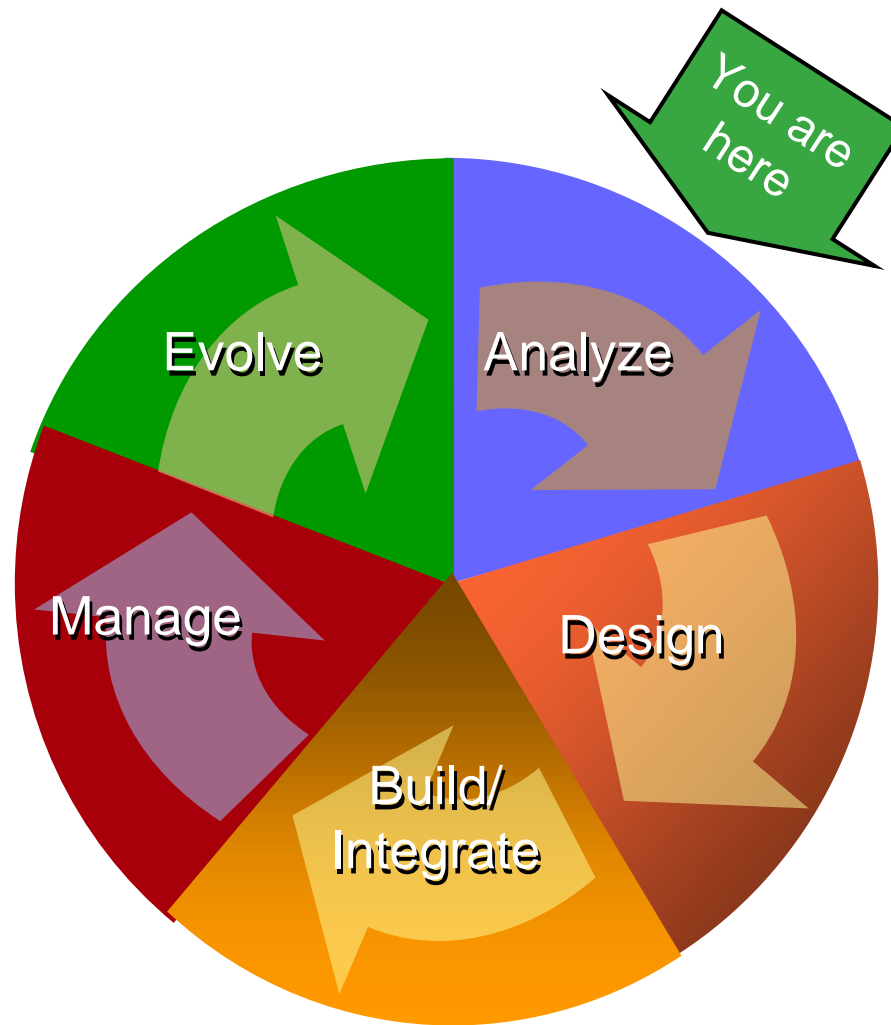
It's a process



Project initiation



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



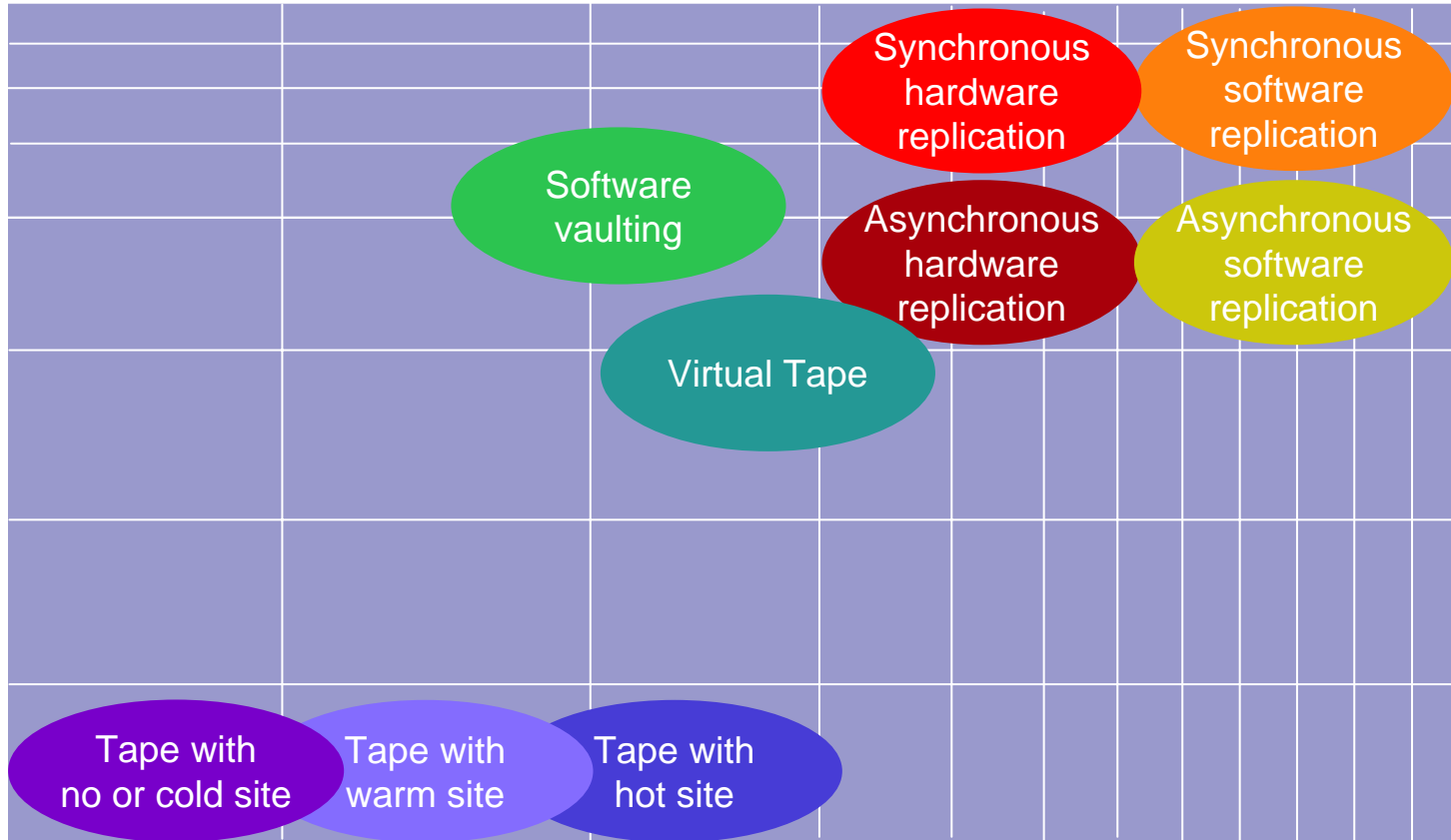
- Risk analysis and controls
- Business impact analysis
 - Recovery Time Objective
 - Recovery Point Objective
- Alternative strategies, cost benefit analysis, and budgeting

Separating RTO and RPO



Continuity

Data loss (RPO)

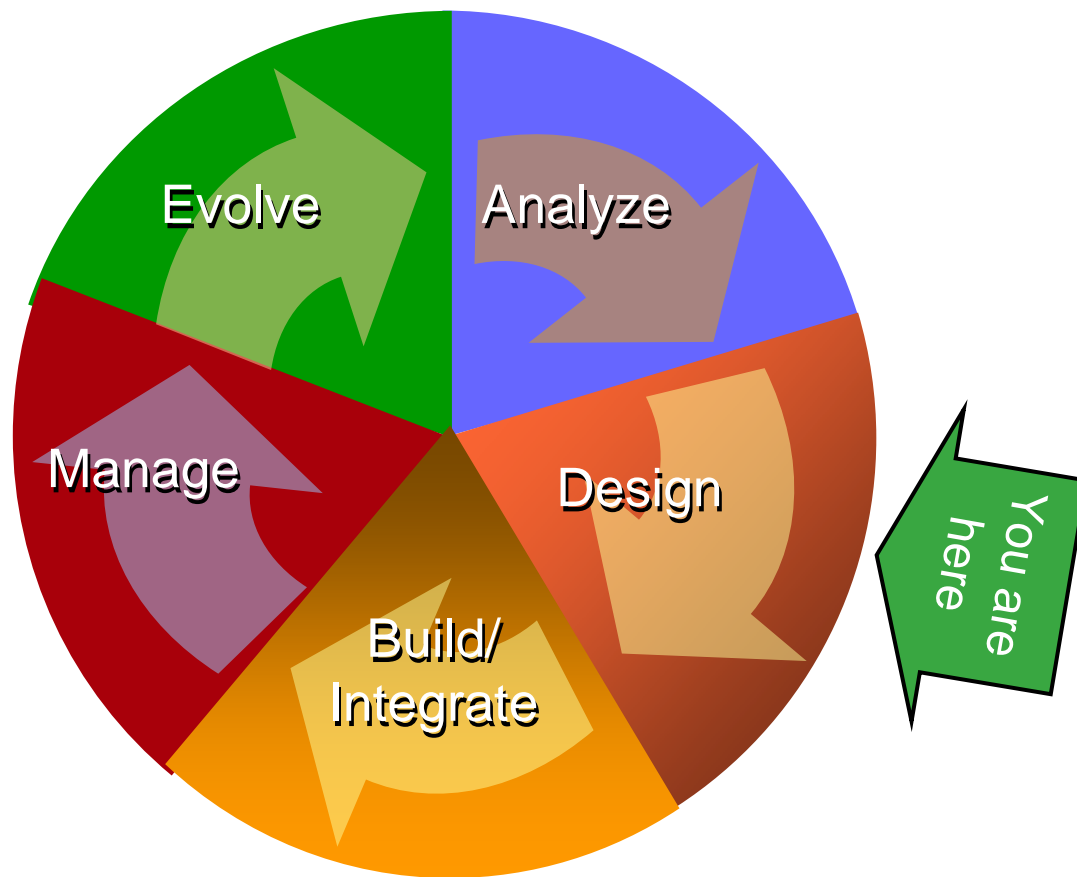


Recovery

Downtime (RTO)

Continuity



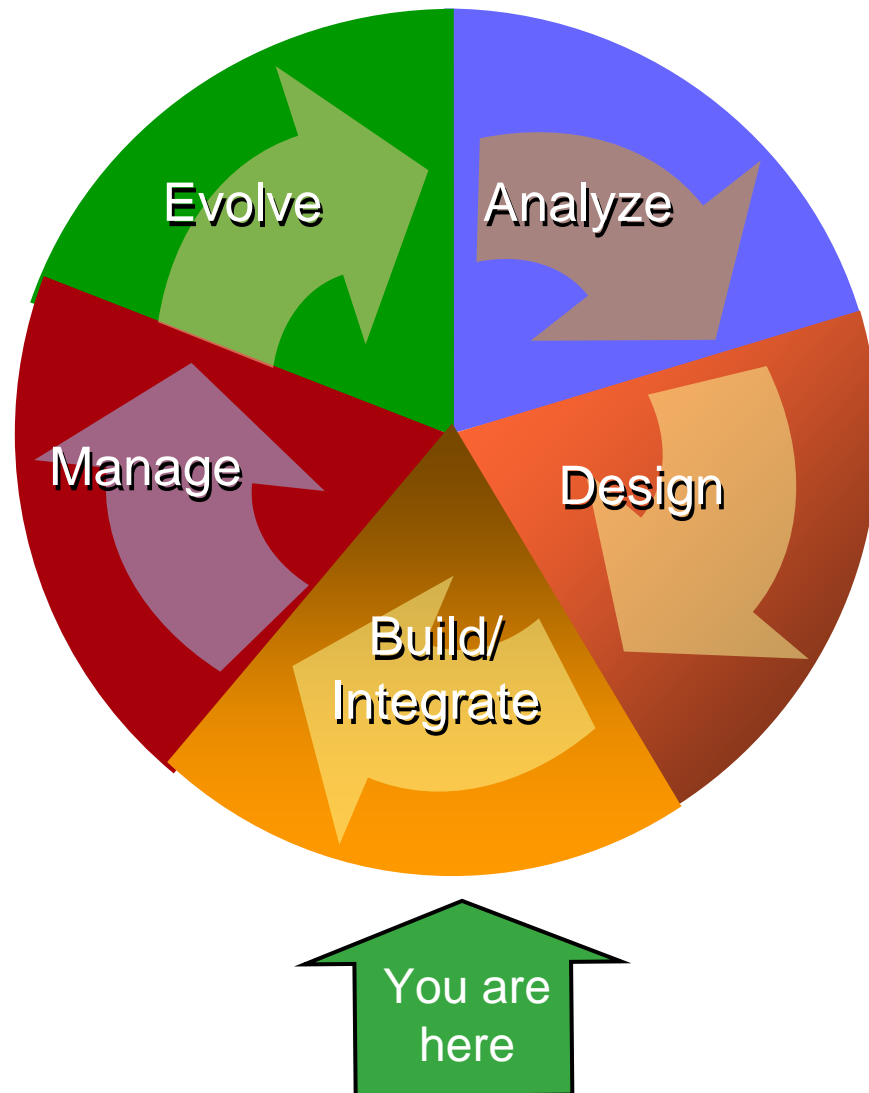


- Scope and objectives
- Deployment teams
- Cookbook
- Key disaster scenario
- Escalation, notification, and activation

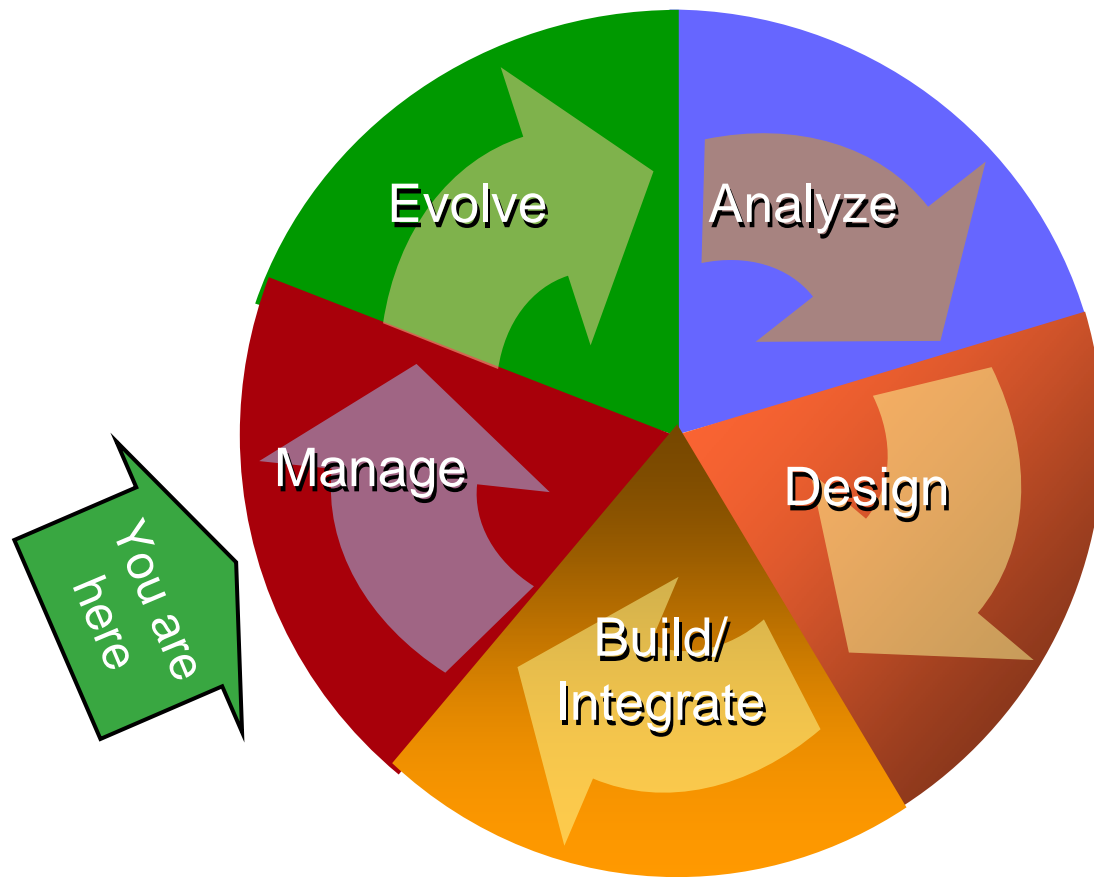
Key disaster scenario:

“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.”





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



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



- 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.

- 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.

IT recovery is not complete without a business continuity plan.



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





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”?

HP Business Continuity services: Size, stability, and global presence



Total number of countries with an HP Business Continuity services presence:

40

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.



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

For more information...



- Useful URL
 - <http://www.hp.com/go/nonstopcontinuity>
- Product manager for continuity products
 - Ron LaPedis, +1 (408) 285 5987
 - ron.lapedis@hp.com



i n v e n t