IBM Global Technology Services

Business Continuity and Resiliency Services

Best Practices for Business Continuity and Disaster Recovery Planning

Paul D. Saxton,
Executive Consultant and Practice Leader

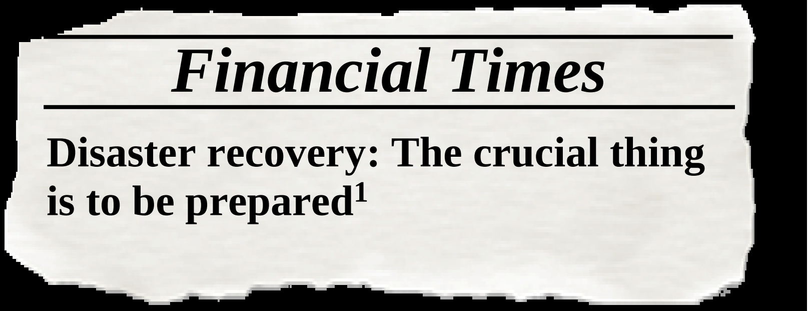
Agenda

- Industry Trends and Directions
- Experiences and Lessons Learned
- Best Practices
- Steps to Consider

Industry Trends and Directions

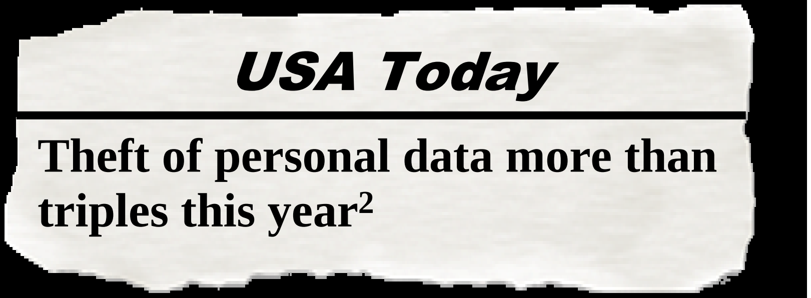
The world is riskier than it used to be ...

- **Changing environment**
  - Expanding risk exposures
  - Increased global and regional interdependencies
  - Supply chain disruption
- **Heightened impact of business disruption**
  - Greater financial implications of downtime
  - Brand vulnerabilities
  - Data integrity requirements
- **More complex regulations**
  - Changing industry and regulatory standards
  - Geographic dispersal requirements
  - Varying regulations per country



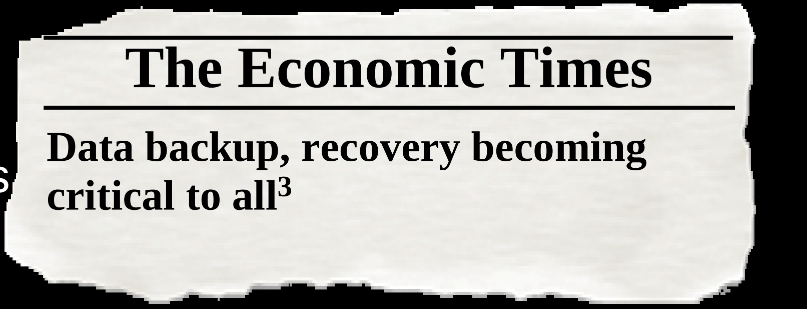
Financial Times

Disaster recovery: The crucial thing is to be prepared[1]



USA Today

Theft of personal data more than triples this year[2]



The Economic Times

Data backup, recovery becoming critical to all[3]

[1] Jane Croft, “Disaster recovery: The crucial thing is to be prepared,” *Financial Times*, May 8, 2007, http://us.ft.com/ftgateway/superpage.ft?news_id=fto050820071017005239

[2] Byron Acohido, “Theft of personal data more than triples this year,” *USA Today*, December 9, 2007, http://www.usatoday.com/tech/news/computersecurity/infotheft/2007-12-09-data-theft_n.htm

[3] Harsimran Singh, “Data backup, recovery becoming critical to all,” *Economic Times*, November 23, 2007, http://economictimes.indiatimes.com/Infotech/Software/Data_backup_recovery_becoming_critical_to_all/articleshow/2563298.cms

…and disruptions have an enormous impact on the business

Industry Sector	Revenue / Hour	Revenue / Employee Hour
Energy	**$2,817,846**	**$ 569.20**
Telecommunications	**$2,066,245**	**$ 168.98**
Manufacturing	**$1,610,654**	**$ 134.24**
Financial Services	**$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**
Food / Beverage Processing	**$ 804,192**	**$ 153.10**
Consumer Products	**$ 785,719**	**$ 127.98**
Chemicals	**$ 704,101**	**$ 194.53**
Transportation	**$ 668,586**	**$ 107.78**
Utilities	**$ 643,250**	**$ 380.94**
Healthcare	**$ 636,030**	**$ 142.58**
Metals / Natural Resources	**$ 580,588**	**$ 153.11**
Professional Services	**$ 532,510**	**$ 99.59**
Electronics	**$ 477,366**	**$ 74.48**
Construction & Engineering	**$ 389,601**	**$ 216.18**
Media	**$ 340,432**	**$ 119.74**
Hospitality & Travel	**$ 330,654**	**$ 38.62**
Average	$1,010,536	$ 205.55

Source: Meta Group, 2004

- Downtime ranges from **300–1,200 hours per year**, depending on industry[4]
- In some industries, downtime costs can equal **up to 16 percent of revenue**[4]
- For **32 percent** of organizations, just four hours of downtime could be severely damaging[5]

[4] Infonetics Research, *The Costs of Enterprise Downtime: North American Vertical Markets 2005*, Rob Dearborn and others, January 2005.

[5] Continuity Central, “Business Continuity Unwrapped,” 2006, http://www.continuitycentral.com/feature0358.htm

It Does Happen

55% of Canadian firms reported a business disruption in the last 12 months.

How many others had problems that were NOT reported?

Source: IDC 2007

And it may not be what you planned for…

Event	Date	Impact
October snowstorm	2006	Dumps 30-60 cm of snow on Niagara Peninsula and eastern Lake Erie knocking out power to thousands of residents
Severe thunderstorms in Muskoka/Huntsville / Haliburton	2006	Widespread damage to power infrastructure for thousands of residents – outages lasting 8 days and more
Hurricane Katrina	2005	Costliest and most deadly natural disaster in US history – Damage estimates exceed $200 billion
Blackout in North America	2003	An estimated 50 million people and thousands of businesses left without power
Malicious computer worm hits 13,000 ATMs at Bank of America	2003	Bank unable to process customer transactions and impacted Internet traffic worldwide
Disintegration of Enron	2001	Affected energy markets worldwide; led to new regulations on corporate financial reporting
Terrorist attacks of September 11th	2001	Impacted financial markets worldwide for over 6 months; led to war on terrorism, revealed weaknesses in recovery plans for hundreds of companies
Hurricane Floyd	1999	Damage estimated at over $6 billion. Set many flood records.
Hurricane Andrew	1992	Damage estimated at $25 billion – Most expensive natural disaster in US history.

… and what's up with the squirrels?

- **Squirrel** blamed for Toronto power outage

  Last Updated: Wednesday, September 19, 2007 , 1:57 PM ET CBC News

  A wayward eastern grey squirrel may be to blame for a power surge Wednesday morning that caused traffic tie-ups in Toronto's downtown core and left parts of the financial district powerless.

- **Squirrel** causes power outage

  Saskatchewan News Network; Regina Leader-Post, Published: Thursday, December 20, 2007

  REGINA (SNN) -- A squirrel on a power line was the cause of a power outage in Regina on Wednesday.

  SaskPower spokesperson Larry Christie said the disruption began just before 10 a.m. and ended about a half-hour later.

  About 500 customers were affected in Regina's Cathedral, Lakeview and Normandy Heights areas. The Regina International Airport also was affected by the outage, but the power disruption didn't cause any delays in flight arrivals or departures.

- Fort Worth boil advisory lifted day after power outage

  12:43 PM CST on Saturday, March 1, 2008, Associated Press

  Fort Worth water officials today lifted a boil-water advisory placed on parts of the city after an electric power outage shut down two water pumping stations.

  A **squirrel** is blamed for the outage yesterday that cut electric power to thousands of customers and prompted the boil-water advisory for parts of southwestern Fort Worth.

… Who knows!

- State of Georgia
  - 5,273 **squirrel** related outages in 2005
  - 16,750 **squirrel** related outages in 2006

Notable Trends

- **Senior level executives seeking proof of recovery capabilities** – lack of confidence that current state reflects true recovery requirements and capabilities.
  - US regulators taking firmer stand, Canadian regulators increasing their focus.
- **Continued focus on moving forward to further mitigate risks to recoverability:**
  - Integrated cross platform recovery – capabilities and testing.
  - Full end-to-end application recovery.
  - Alignment of recovery capabilities with business requirements & expectations.
  - Formalized governance models to facilitate integration, consistency and reduction in "tower or silo" mentality.
  - Adopting business resilience strategies for continuity of operations vs traditional failure/recover/resume strategy.
  - Work area recovery for end users (centralized and mobile).
  - Pandemic preparedness.
  - Integrating BCP/DR/Crisis Management.
  - Increased focus on Regulatory compliance.
  - Management of BCP/DR documentation – consolidated centrally managed repositories.

A perplexing array of regulations touch BCP, DR and Resilience

Organizations need to understand the ones they are obliged to comply with as well as the ones they choose to adopt.

International Regulations

- Basel I
- Basel IA
- Basel II
- Solvency II
- European Privacy Acts
- Statute of the European System of Central Banks
- Commission of European Communities OECD Principles
- Markets in Financial Instruments Directive (MiFID)
- UK’s Financial Services Authority Combined Code, includes Turnbull Guidance and COSO
- Australia’s Stock Exchange (ASX) Principles
- Japan’s JSOX
- India’s Clause 49, Right of Information Act 2002
- Germany’s KonTraG 1999
- Canada’s CSOX (52-109 and 52-111)
- Islamic Banking Law

ASX
AUSTRALIAN STOCK EXCHANGE

BANK FOR INTERNATIONAL SETTLEMENTS

CEA

OECD

OSC
Ontario Securities Commission

FSA

US Regulations

- Anti-Money Laundering Laws and Regulations
- Anti-Tying
- Community Reinvestment Act (CRA)
- Federal Reserve Regulation
  - Sections 23A and 23B
  - Covered Borrowers, Regulation U, T
  - Section 214 – Relations with Foreign Banks
- Federal Deposit Insurance Corporation Improvement Act (FDIC)
- Gramm-Leach-Bliley Act (GLBA)
  - Financial Holding Company (FHC)
    - Banking activities plus expanded activities that include
      - securities underwriting and dealing
      - insurance agency and underwriting activities; and
      - merchant banking activities
  - Bank Holding Company Act
- Public Company Accounting Oversight Board (PCAOB)
- Department of Treasury, Office of the Controller of the Currency (OCC)
- Securities and Exchange Commission, Consolidated Supervised Entities (CSE)
- Sanctions, Congressional or executive order
- Sarbanes-Oxley Act (SOX), Sections 302, 401, 403, 404, 406, 408, 409,…….
- US Anti-Boycott Regulations
- US Export Controls
- US Foreign Corrupt Practices Act (“FCPA”)
- USA Patriot Act
- Confidentiality, Conflicts of Interest, Personal Investments, Chinese Walls
- Customer Suitability / Appropriateness

Canadian Regulations

- CAN / CSA-Z1600 Emergency Management and Business Continuity
- Treasury Board Secretariat – Management Accountability Framework (MAF)
- Emergencies Act (Fed)
- Emergency Program Act (BC), Emergency Measures act (MB), Emergency Management Act (ON)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Patriot Act
- Office of the Superintendent of Financial Institutions (OSFI)
- Canadian Banking Association
- Investment Dealers Association

CANADIAN STANDARDS ASSOCIATION

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Investment Dealers Association of Canada

Association canadienne des courtiers en valeurs mobilières

Manitoba

British Columbia

The Best Place on Earth

Ontario

Treasury Board of Canada Secretariat

Securities and Exchange Commission MCMXXXIV

Multiple and Diverse Best Practice Frameworks

- International Risk Governance Council (IRGC)
- Federation of European Risk Management Associations (FERMA)
- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
  - 1992, Internal Control Framework
  - 2004, Enterprise Risk Management Framework (ERM)
- Information Systems Audit and Control Association (ISACA)
  - Control Objectives for Information and related Technology (COBIT)
- IT Governance Institute (ITGI)
- International Organization for Standardization (ISO)
  - ISO/IEC 17799, ISO/IEC 27002:2005 expected to be renamed ISO/IEC 27002:2007
- British Standards Institute (BSI), BS 7799-1:1999, BS 7799-2:2002, BS 25999
- Business Continuity Institute
- Disaster Recovery Institute International
- Generally Accepted Accounting Principals (GAAP) – Financial Reporting Standards (FRS)
  - International Accounting Standards (IAS) – International GAAP
  - Financial Accounting Standards Board (FASB) - US GAAP
  - Local Reporting Standards – Local GAAP
- Extensible Business Reporting Language (XBRL)

irgc

XBRL®
eXtensible Business Reporting Language

ferma
Federation of European Risk Management Associations

ISACA
Serving IT Governance Professionals

BSi

ISO
International Organization for Standardization

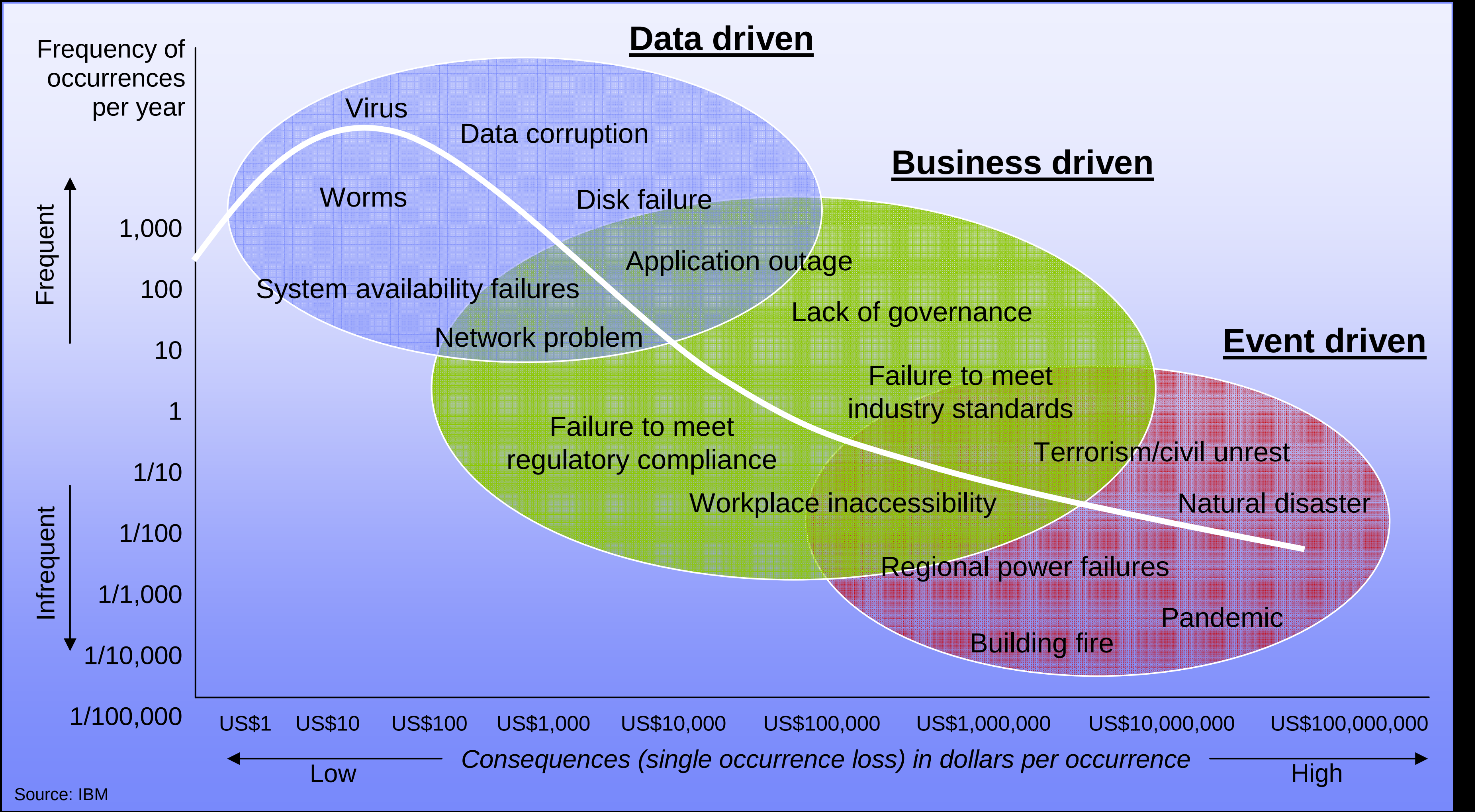
International Accounting Standards Board®

IT GOVERNANCE INSTITUTE®

FASB FINANCIAL ACCOUNTING STANDARDS BOARD

Experiences and Lessons Learned

Focus to date on frequent events that are easy/inexpensive to address



Source: IBM

Lessons Learned: September 11, 2001

- No prior experience
- Entire world did not grind to a halt
- Need to plan for the worst case scenario
  - Loss of entire business operation and impact of the crisis
  - Personnel, Vital Records, Network, Systems
- Evaluate true risk exposure in continuity plan
- Mismatch between business requirements and recovery plan
- Lack of Crisis Response Plans (safety, salvage, communications, command & control)
- Recovery plan did not cover all critical business functions
- Undersubscribed Contracts
  - ISP Connections, End User Work Area, DASD, Print, Fax, CPU Capacity

Lessons Learned: September 11, 2001

- No alternate staff available to implement recovery plans
- Documented procedures untested and out of date – contained incorrect information
- Communications
  - Web site recovery insufficient
  - Reliance on email underestimated
- No plans to reroute surface mail
- No plans to reroute voice services
- No plans for external and internal communications to employees, business partners, vendors, etc...
- Need plans to continue operations past traditional 6 week hot site contract
- Rebuilding the business from ground up
- Transition of operations from recovery center to back home

Lessons Learned: March 2003 SARS

- No prior experience
- Government slow to react
- Reaction not uniform
- Optics had higher impact than actual outbreak
- Rumours and mis-information fueled concerns
- Rolling outage for weeks/months
- HR policies did not support continuity / crisis plans
- Employees not informed of special policies regarding infectious outbreak – weak communication plans
- Lack of crisis command centre / war room facilities
- Many companies didn’t have a plan
- Fear played an important role

Lessons Learned: August 2003 Power failure

- People and families took priority
- Staggered restoration of services slowed recovery
- Supply chain failures felt immediately - cash, fuel, food, water
- Data delivery issues - Traffic jams, vendor issues, fuel for trucks
- Entire world did not grind to a halt
- Other people’s problems became your problems
- Cellular service not designed for regional failures
- Widespread nature affecting “everyone” lessened overall impact to individual firms
- Occurred at “best” vs “worst” possible time – we were very lucky!
- Realization that previous “lessons learned” were not applied

Lessons Learned: 2005 Katrina

- Business Continuity still being overlooked
  - People are the most important element
    - Where will they work? How will they get there?
    - What about families? What about basic needs?
- Business Continuity must include ALL your business partners
- Make sure ALL of your essential software is current and under maintenance
- Test after every hardware change and rotate through testers
- Need user executive/manager responsible for user plan
- Always bring users when testing
- Planning to return is as important as planning recovery
- Management must decide on and document policies concerning
  - Pay
  - Travel and living expenses
  - Plan what help your company will give employees
  - Plan on how to locate and communicate with employees

Summary: More attention to resilience is needed across the enterprise

Mismatch exists between business requirements and recovery plans / capabilities

The most important impacts are often the hardest to measure

Plans developed do not consider the impact across the organization (silo based)

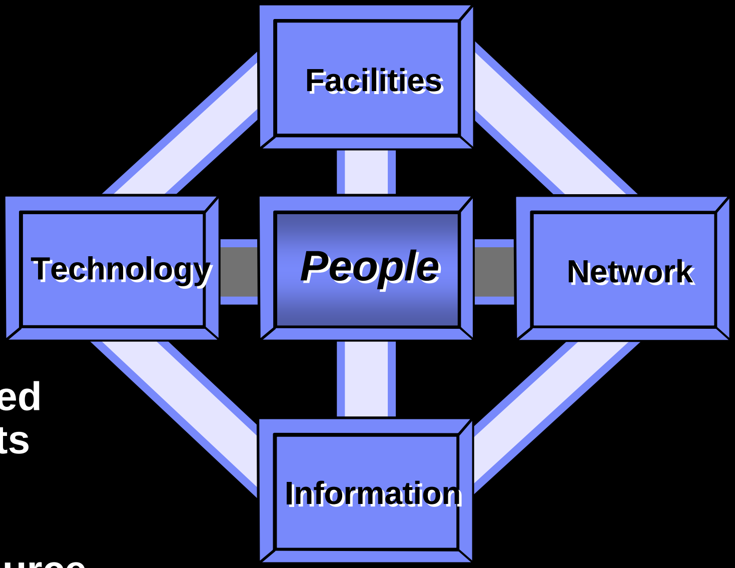
Plans are not exercised or maintained at appropriate levels of detail

Internal and/or external communications processes are not crisp

Documentation is scattered all over in pieces and parts

Insufficient time and resource available to properly test

Major disruptions to availability of human capital resources not previously considered



Network availability can be a major bottleneck in restoring business operations

Plans do not effectively address the impacts of a regional emergency

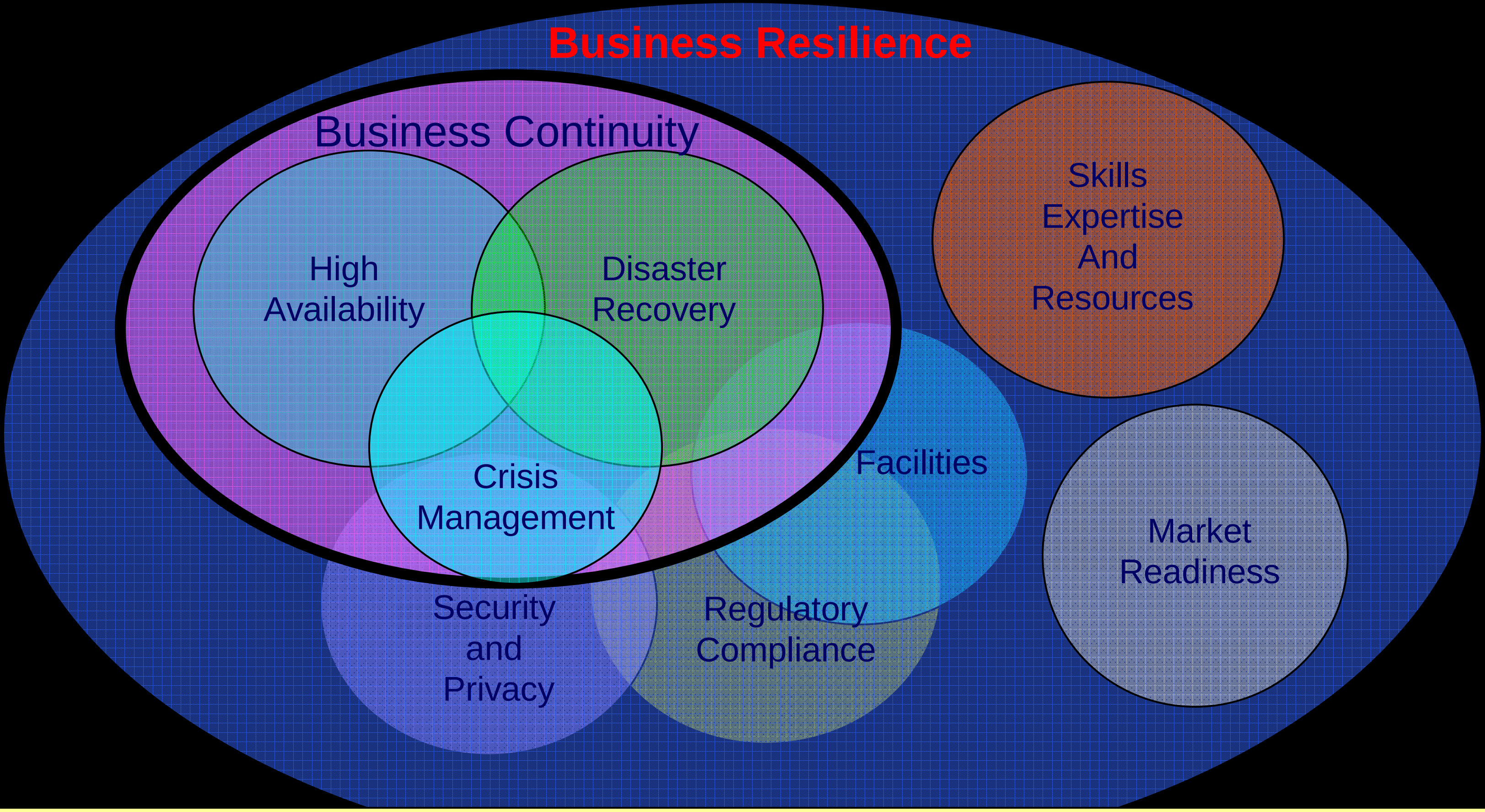
Dependency on key personnel not properly addressed in plans

Lack of governance, policy and standards results in disorganized program implementation

Fragmented program ownership and lack of governance are root causes

Best Practices

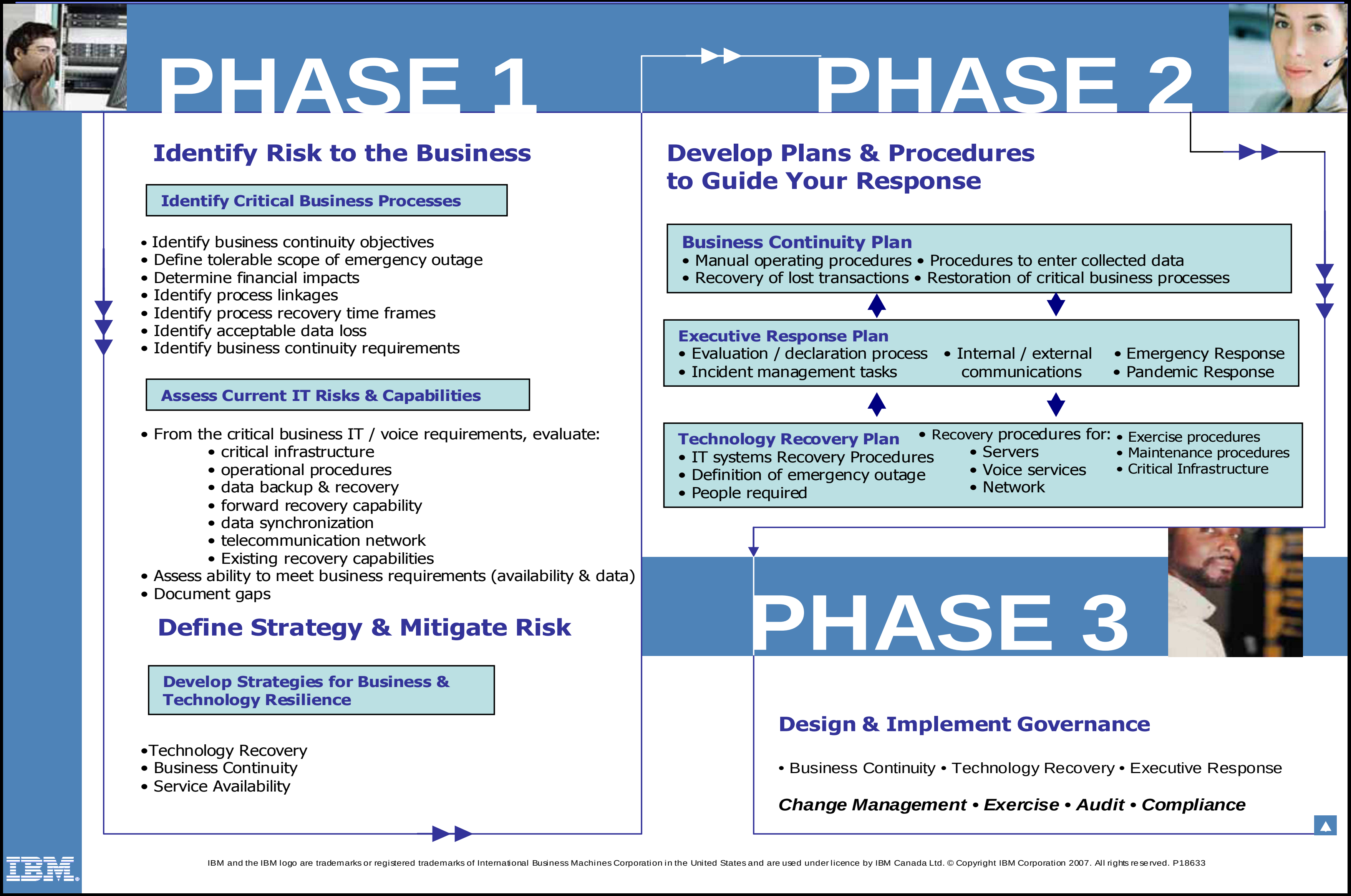
Think of Resilience at the enterprise level – not just IT



Business Continuity is the ability of an organization to ensure continuity of service and support for its customers, employees and business partners and to maintain its viability before, during and after an event.

Business Resilience is the ability of an enterprise to rapidly adapt and respond to risks, as well as opportunities, in order to maintain continuous business operations, be a more trusted partner, and enable growth.

Easy to understand, hard to implement – A proven methodology helps



PHASE 1

Identify Risk to the Business

Identify Critical Business Processes

- Identify business continuity objectives
- Define tolerable scope of emergency outage
- Determine financial impacts
- Identify process linkages
- Identify process recovery time frames
- Identify acceptable data loss
- Identify business continuity requirements

Assess Current IT Risks & Capabilities

- From the critical business IT / voice requirements, evaluate:
  - critical infrastructure
  - operational procedures
  - data backup & recovery
  - forward recovery capability
  - data synchronization
  - telecommunication network
  - Existing recovery capabilities
- Assess ability to meet business requirements (availability & data)
- Document gaps

Define Strategy & Mitigate Risk

Develop Strategies for Business & Technology Resilience

- Technology Recovery
- Business Continuity
- Service Availability

PHASE 2

Develop Plans & Procedures to Guide Your Response

Business Continuity Plan

- Manual operating procedures
- Procedures to enter collected data
- Recovery of lost transactions
- Restoration of critical business processes

Executive Response Plan

- Evaluation / declaration process
- Incident management tasks
- Internal / external communications
- Emergency Response
- Pandemic Response

Technology Recovery Plan

- IT systems Recovery Procedures
- Definition of emergency outage
- People required
- Recovery procedures for:
  - Servers
  - Voice services
  - Network
- Exercise procedures
- Maintenance procedures
- Critical Infrastructure

PHASE 3

Design & Implement Governance

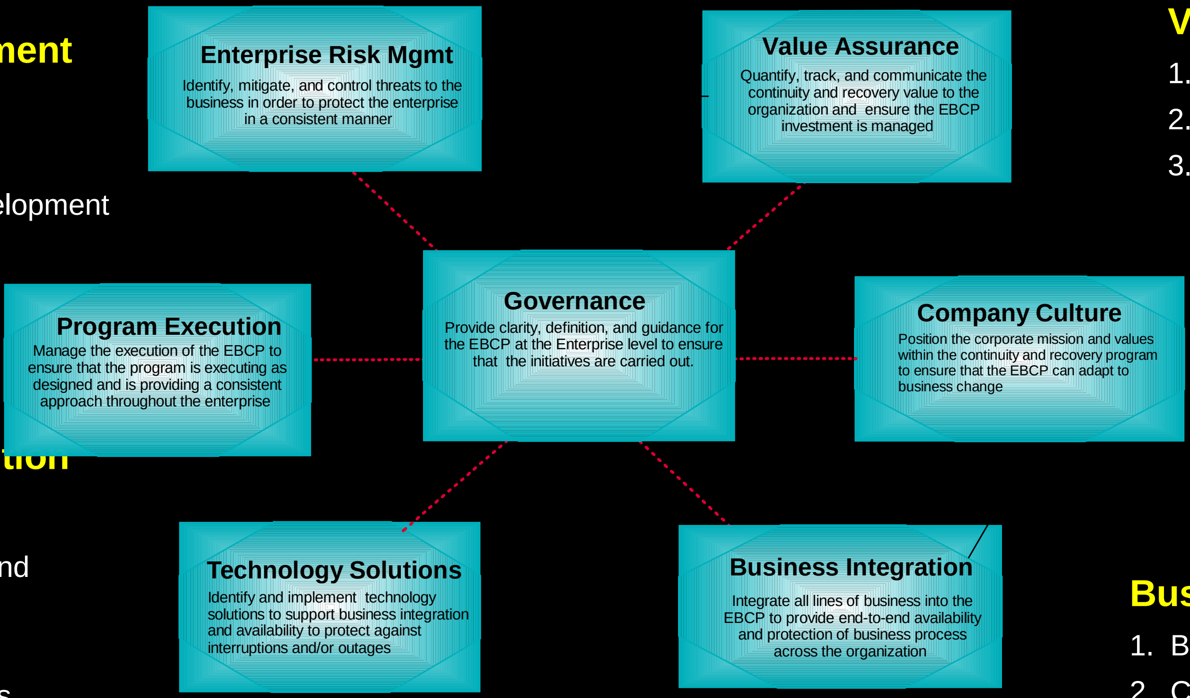
• Business Continuity • Technology Recovery • Executive Response

Change Management • Exercise • Audit • Compliance

Applying the methodology to a robust Resilience Framework enables the integration of 7 key areas with defined critical success factors

Risk Management

1. Identification
2. Quantification
3. Response Development
4. Risk Control



Enterprise Risk Mgmt

Identify, mitigate, and control threats to the business in order to protect the enterprise in a consistent manner

Value Assurance

Quantify, track, and communicate the continuity and recovery value to the organization and ensure the EBCP investment is managed

Governance

Provide clarity, definition, and guidance for the EBCP at the Enterprise level to ensure that the initiatives are carried out.

Program Execution

Manage the execution of the EBCP to ensure that the program is executing as designed and is providing a consistent approach throughout the enterprise

Company Culture

Position the corporate mission and values within the continuity and recovery program to ensure that the EBCP can adapt to business change

Technology Solutions

Identify and implement technology solutions to support business integration and availability to protect against interruptions and/or outages

Business Integration

Integrate all lines of business into the EBCP to provide end-to-end availability and protection of business process across the organization

Value Assurance

1. Initiative Selection
2. Initiative Monitoring
3. Value Measurement

Corporate Culture

1. Vision and Mission
2. Capacity for Change
3. Values

Program Execution

1. Planning
2. Communication and Integration
3. Funding
4. Human Resources

Business Integration

1. Business Impact
2. Critical Resource Identification
3. EBCP Maintenance
4. Recovery Objectives
5. Audit Controls / Regulatory Compliance
6. Vital Records Protection
7. Information Management

Technology Solutions

1. Strategic Planning
2. Operations / Management
3. Validation
4. Data Management

Governance

1. Enterprise Strategy
2. Corporate Continuity Policy
3. Cross Functional Teaming
4. Executive Communications
5. Role and Responsibility Definition

IBM has also developed a Model to help illustrate who does what across the entire organization – not just within IT

STRATEGY & VISION

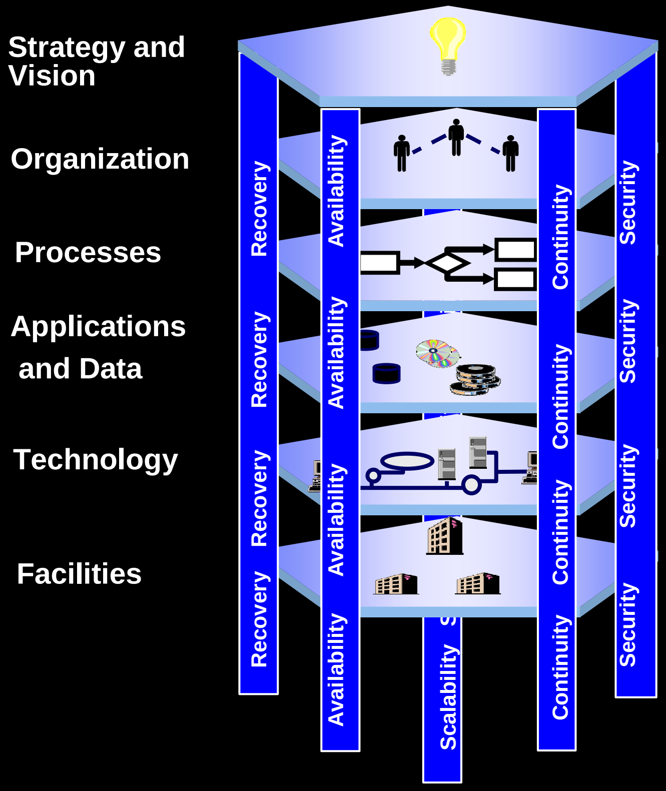
- Governance strategy
- Financial strategy
- Communications strategy
- New product/services strategy
- Risk management

APPLICATIONS and DATA

- Data security
- Data storage
- Application architecture and design
- Backup and recovery

TECHNOLOGY

- Hardware architectures
- System software
- Middleware
- Networks



PROCESSES

- Business Process
  - Sales Order
- Financial
  - CRM
  - Claims processing
  - Business controls
  - Quality Management
  - Research & Development
  - Enterprise Resource Planning
- IT Process
  - Change management
  - Problem management
  - Incident management
  - Availability management

ORGANIZATION

- Roles & Responsibilities
- Structures
- Skills
- Cross-organizational cooperation

FACILITIES

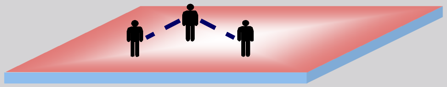
- Physical and logical security
- Safeguard access
- Power protection
- Environmental considerations

Resilience implementation varies across an enterprise matching capabilities with requirements at various levels

Strategy and vision

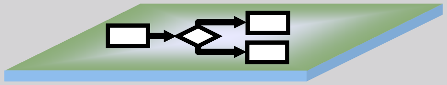
- Crisis management process
- Executive knowledge of resilience capabilities
- Change management process
- Articulated governance model
- Supplier awareness of requirements
- Resilience used as competitive advantage
- Clearly articulated security policy

Organization



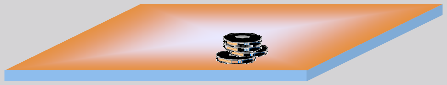
- Geographic diversity of staff
- Call trees and notification
- Backups of workstation data
- Articulated roles and responsibilities
- Identified command center

Processes



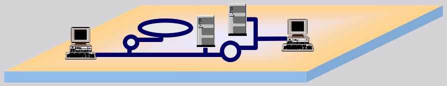
- Identification of most critical processes
- Integrated contingencies
- Split of phone support/call center
- Split of functions
- Key links with external companies
- IT Infrastructure Library® (ITIL®) and Control Objectives for Information and related Technology (COBIT) standards implemented
- Integration into help desk/monitoring

Applications and data



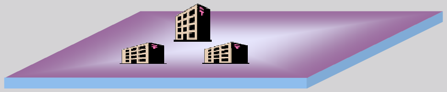
- Replication of critical data
- Remote data backup
- Regular audit of backup
- Service-oriented architecture
- Information lifecycle management
- Database (IBM DB2® software, Oracle) failover and standby
- Identity management
- Information protection
- E-mail filtering and recovery

Technology



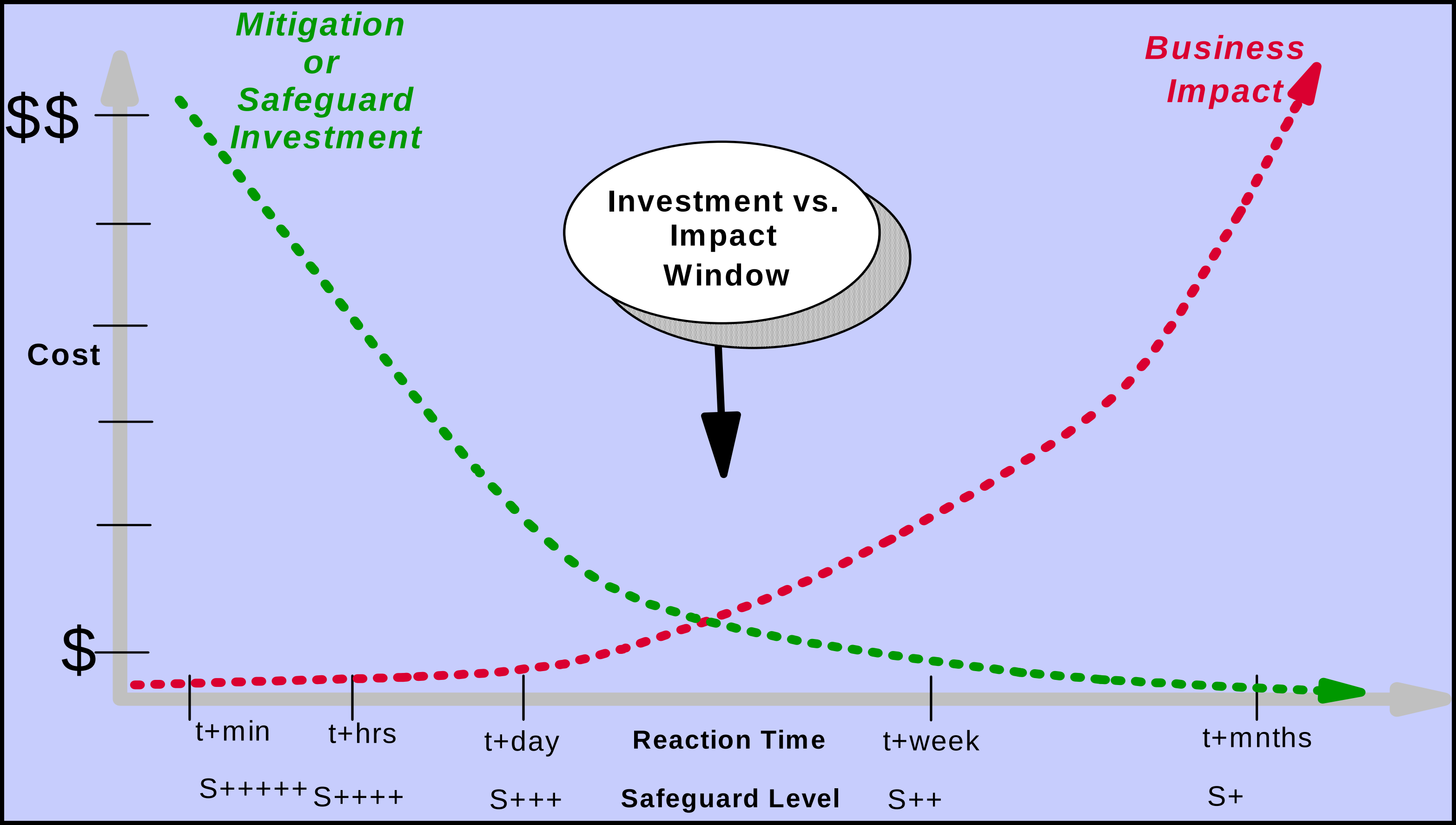
- Mirror login and authentication
- IBM Geographically Dispersed Parallel Sysplex™ (GDPS®) technology for mainframe
- High availability cluster multiprocessing
- Blade servers—dynamic configuration
- Availability of extra components
- Grid computing for high-intensity applications
- 24x7 monitoring of intrusion detection system (IDS) logs

Facilities

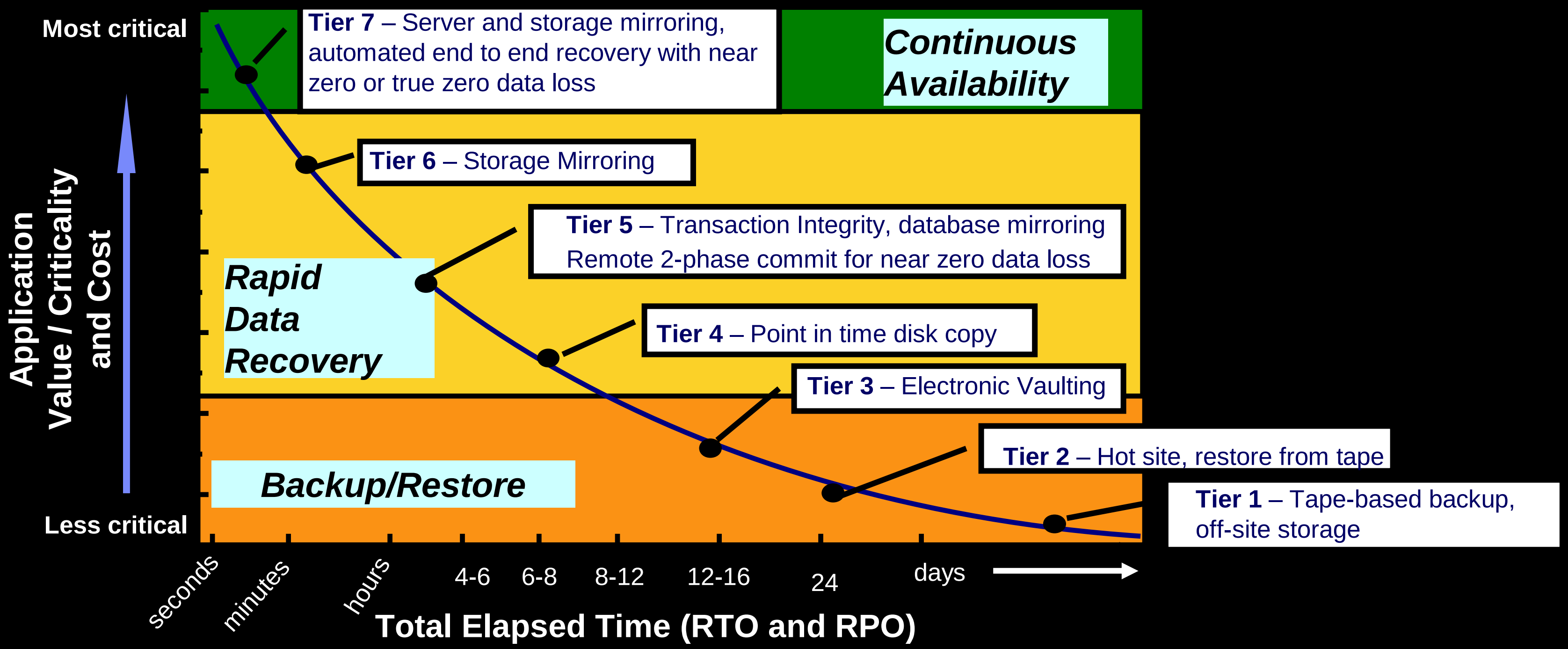


- Diverse power sources
- Diverse network access points
- Uninterruptible power supply (UPS) with two-plus hours
- Diesel generator
- Secondary location more than 50 miles away
- Managed 24x7 physical security
- Biometrics

A corporate resilience strategy should balance the cost of downtime with the cost of uptime



Multiple levels of recovery capability are aligned with varying business operations continuity requirements

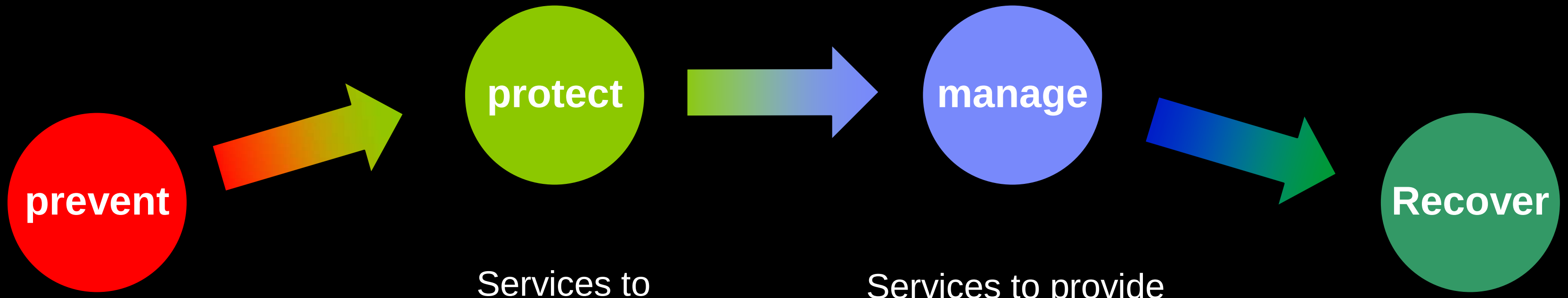


RTO = Recovery Time Objective (how quick is the recovery)

RPO = Recovery Point Objective (how recent is the recovered data)

- Best practice is to blend tier solutions to match requirements (current plus growth).
- One size, one technology, or one methodology does not fit all.
- Solutions can be internal, external or both.

A portfolio of services is needed to support an integrated resilience strategy to help minimize downtime and maximize availability



Services to assess, design and plan for a resilient business infrastructure

Services to remotely store, protect and recover vital business information

Services to provide fault-tolerant, failure-resistant infrastructure with near-zero recovery times

Services to recover business and technology following a negative event

Organizations need to reduce risks to the business by implementing a holistic strategy

1

Improve business resilience

- *Reduce risks and protect confidential intellectual property*
- *Minimize and control impact of planned and unplanned disruptions*

2

Enhance security across your IT

- *Protect critical assets and reduce costs by preempting threats*

3

Implement effective governance

- *Improve service management visibility, control and automation*
- *Align service investments with business priorities*
- *Improve support of governance and compliance requirements*

Summary of steps to consider

1. Analyze risks to the business in the context of continuity, operations, governance and compliance and understand the impact to the enterprise

2. Document availability requirements by business process and applications based on reach, range and overall business value

3. Use a framework that takes a comprehensive approach to analyzing the six resilience layers and uncovering potential points of failure requiring action

4. Implement actions to minimize the frequency, duration and scope of downtime resulting from potential points of failure

5. Formulate a comprehensive resilience strategy that documents how you will:
   - Manage business risk
   - Protect your data
   - Recover from events

6. Regularly review and update your resilience strategy as business requirements change

Get help if you need it – this stuff is not easy to do

IBM Global Technology Services

Thank you

Please contact me directly at:

psaxton@ca.ibm.com

905-316-5410

Or visit us at www.ibm.com/itsolutions/businesscontinuity

Copyright information

IBM Global Services
Route 100
Somers, NY 10589 U.S.A.

Use of the information herein is at the recipient's own risk. Information herein may be changed or updated without notice. IBM may also make improvements and/or changes in the products and/or the programs described herein at any time without notice.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.