2014 ACIIA CONFERENCE
BALI, INDONESIA

ASIAN CONFEDERATION OF INSTITUTE OF INTERNAL AUDITORS

The Stones Hotel - Legian, Bali

24 - 25 November 2014

The Institute of Internal Auditors Indonesia

Organized by:

Supported by:

Crisis Management

A Senior Executive Perspective

Jos Luhukay, PhD
Arghajata Consulting

Bali, 25 November 2014

Topics

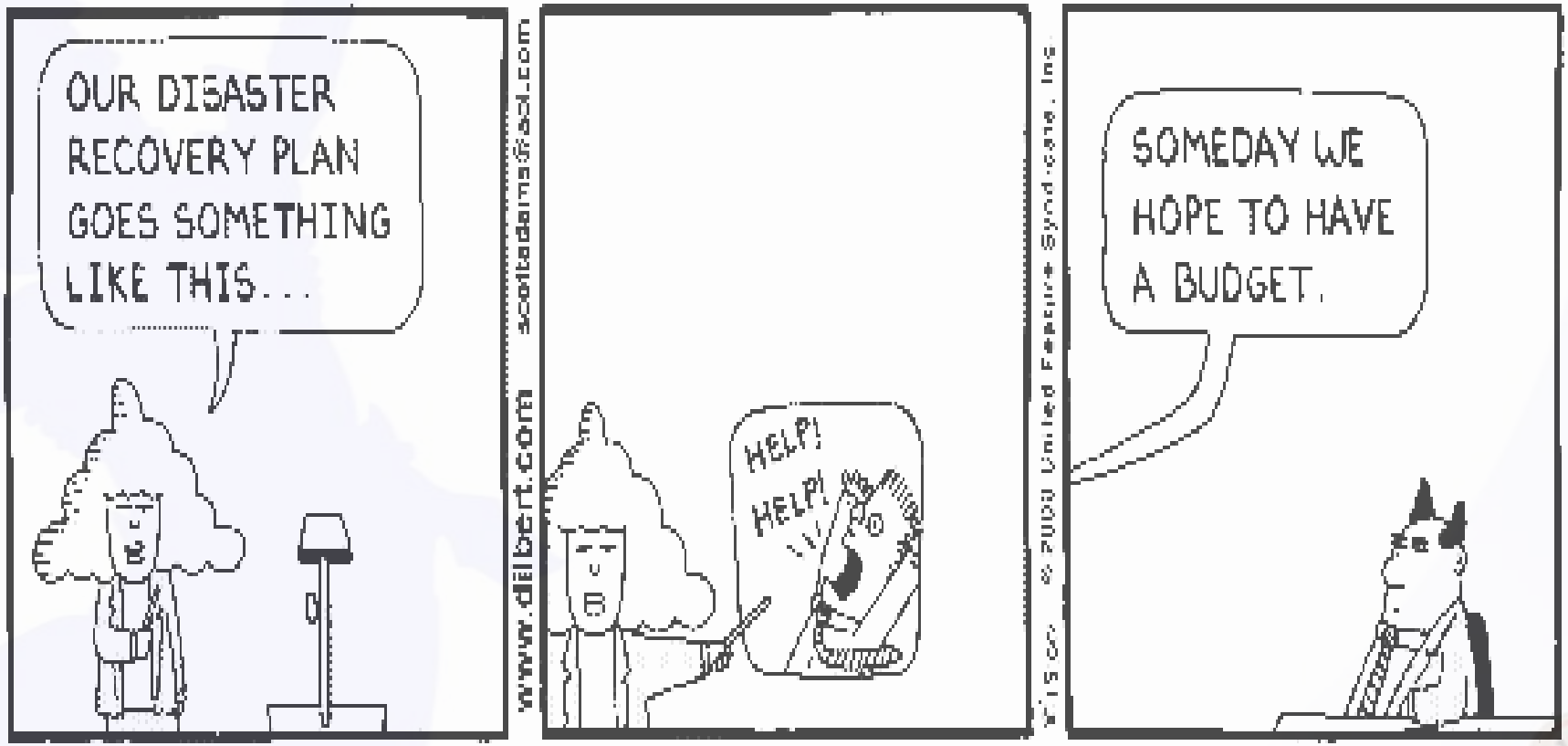
- General Background
- Business Continuity Management
- Management Perspectives
- Caveats

Reference, a.o.: Business Resilience, presented by Scott Ramsey (IBM USA)- 27 May 2009

Topics

- General Background
- Business Continuity Management
- Management Perspectives
- Caveats

Managing Business Crises



Business Continuity Management:
A Definition

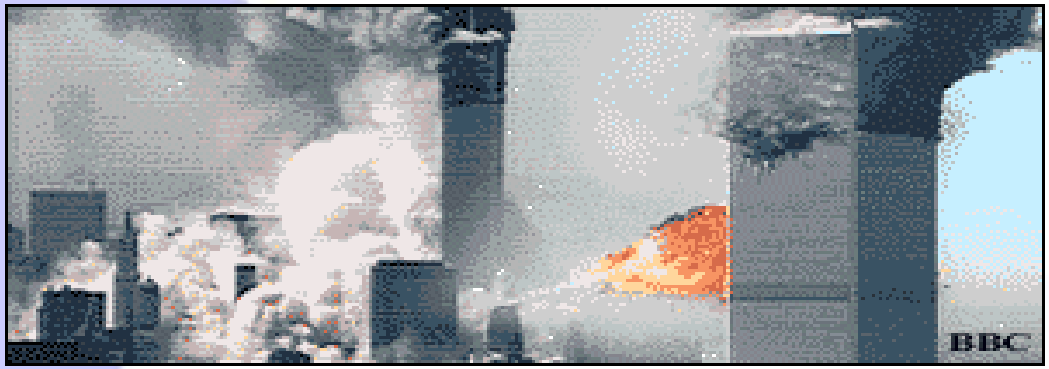
"Fundamentally, BCM seeks to mitigate the impact of a disaster by ensuring alternative mission-critical capability is available when disaster strikes. BCM seeks to preserve the assets of an organization in the event of a disaster: its capability to achieve its mission; its operational capability; its reputation and image; its customer base and market share; its profitability"

Andrew Hiles: "The Definitive Handbook of Business Continuity Management" John Wiley & Sons 1999.

What is a Crisis?

"A crisis is any unplanned circumstance which eventually interferes with a part of the operational or functional environment to the extent that it jeopardizes the company's existence as an on-going concern"

XYZ Coy – Corporate Policy Manual



Types of Crises

- Man-made: fraud & similar improprieties, theft of critical documentation or equipment, terrorism, human error, loss of critical staff, industrial action, demonstrations
- Technical: hardware/software/netware failures, computer viruses, power failures, air-conditioning failure
- Natural: earthquakes, floods, fires, disease outbreaks

Crisis Management and BCM

- **Rule #1: Design and implement the systems so that crisis can be prevented**
- Crisis Management: the first stage in an overall BCM procedure when an incident occurs and requires the immediate response to an incident:
  - Sample case: Power failure in the data center, now what?
- BCM: the overall procedure, comprising planning and then implementation of processes, including CM, which allow the implementation of recovery strategies so as to minimize:
  - Potential loss of life/impact on staff
  - Impacts on customer service levels
  - Financial losses
  - Impacts on reputation

Technology Risk Management (TRM):
An Important Role in the Overall Risk Management Scheme

Technology Risk is a key component of operational risk:

"any adverse outcome, damage, loss, disruption, violation, irregularity or failure arising from the use of or reliance on computer hardware, software, electronic devices, online networks and telecommunications systems"

Source: BIS, Monetary Authority of Singapore

Risks such as associated with:

– **processing errors**	– **control weaknesses**
– **systems failures**	– **security shortcomings**
– **software defects**	– **malicious attacks**
– **operating mistakes**	– **hacking incidents**
– **hardware breakdowns**	– **fraudulent actions, and**
– **capacity inadequacies**	– **inadequate recovery capabilities**
– **network vulnerabilities**	

The Cost of Downtime

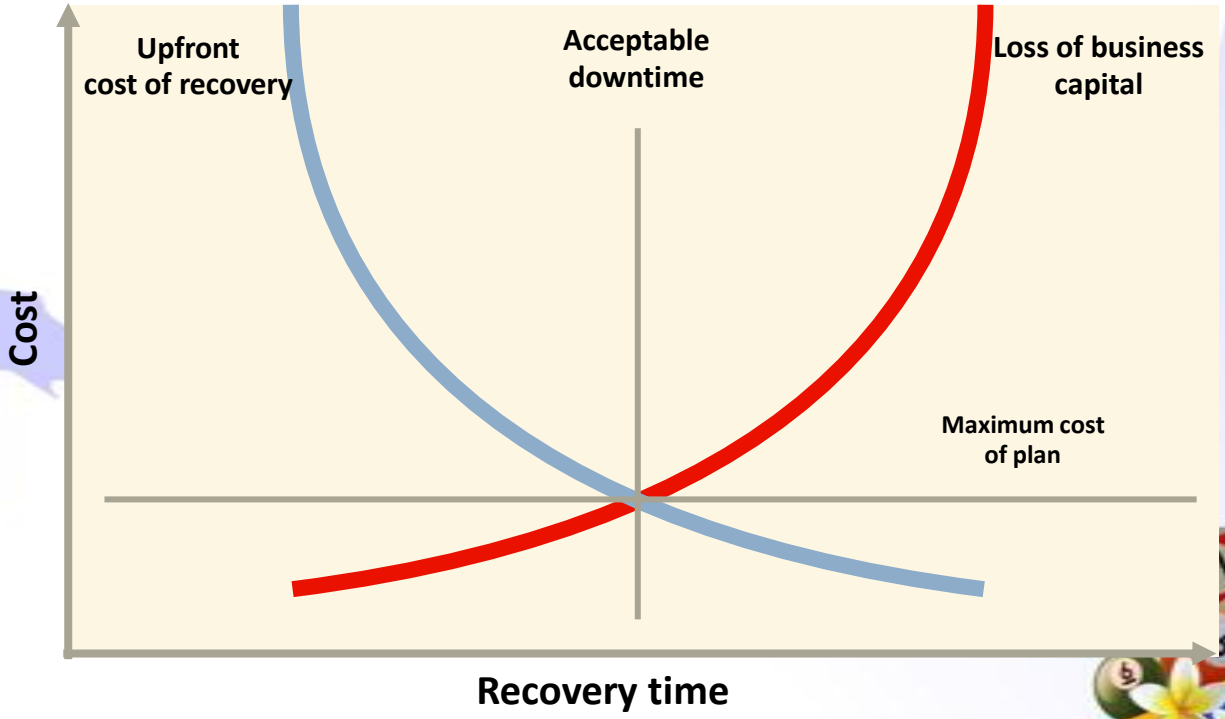
Productivity
- Number of employees impacted **x** hours down **x** burdened hours **=** cost of lost productivity

Financial performance
- Revenue recognition
- Cash flow
- Lost discounts
- Payment guarantees
- Credit rating
- Stock price

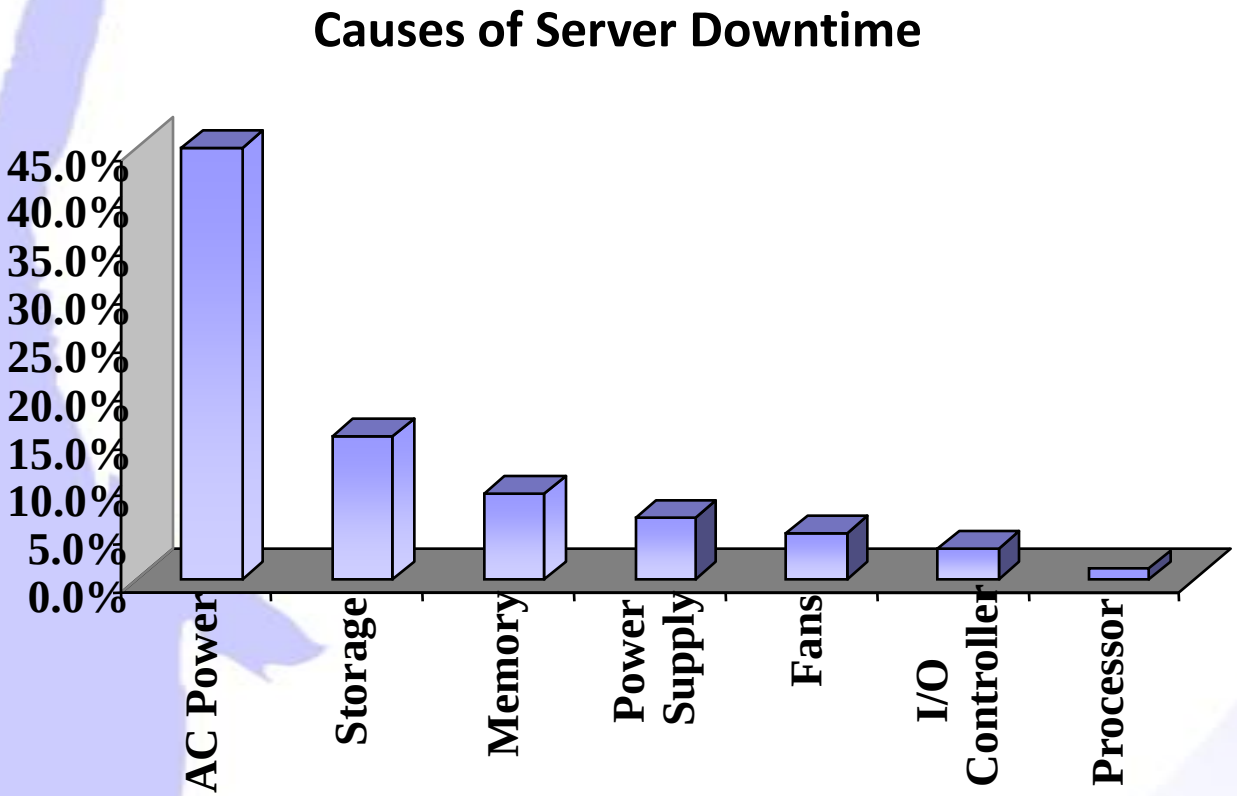
Revenue
- Direct loss
- Compensatory payment
- Lost future revenues
- Billing loss
- Investment loss

Reputation
- Customers
- Suppliers
- Financial markets
- Banks
- Business partners

Other
- **Loss of life**
- **Overtime**
- **Equipment rental**
- **Travel**

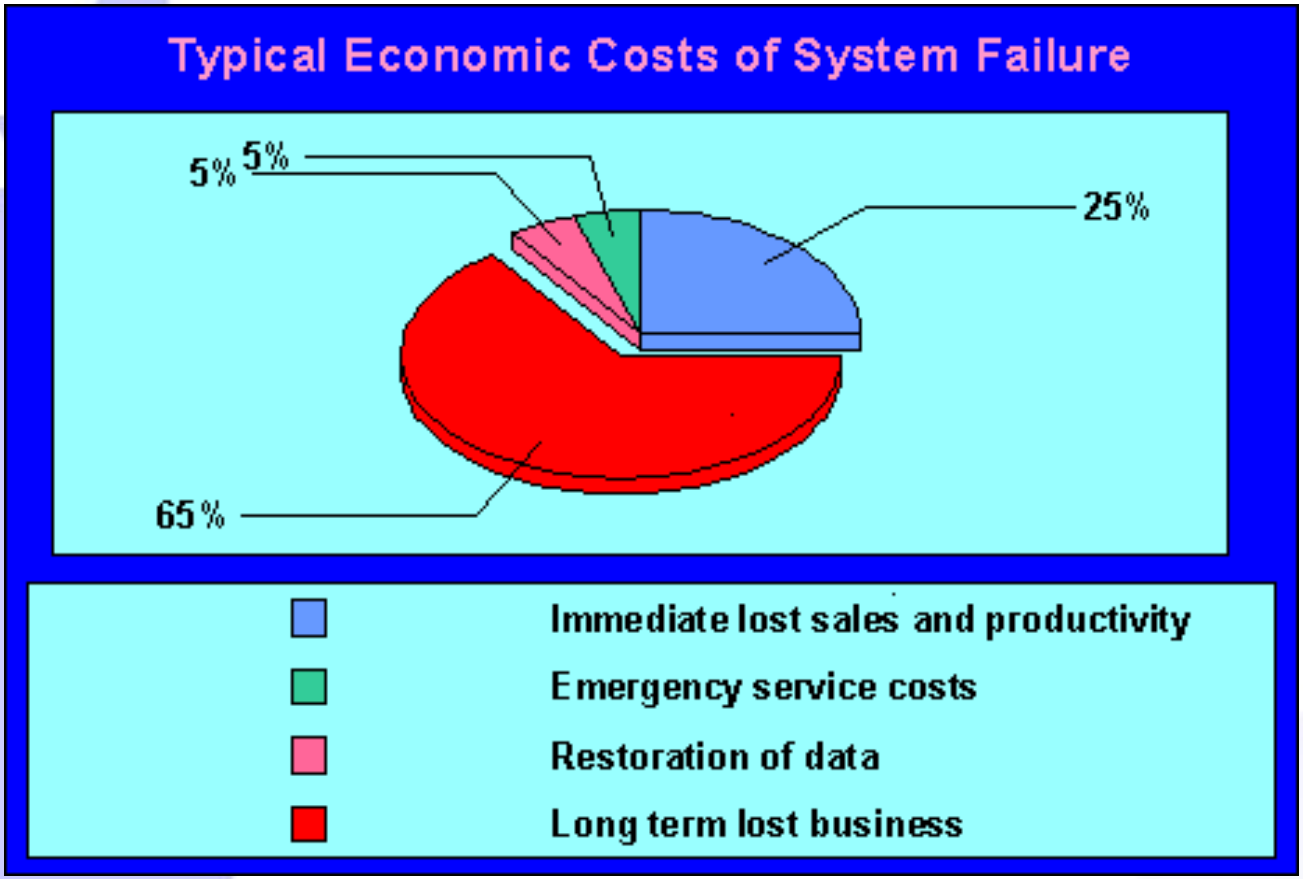


Power Problems Significantly Affect Availability



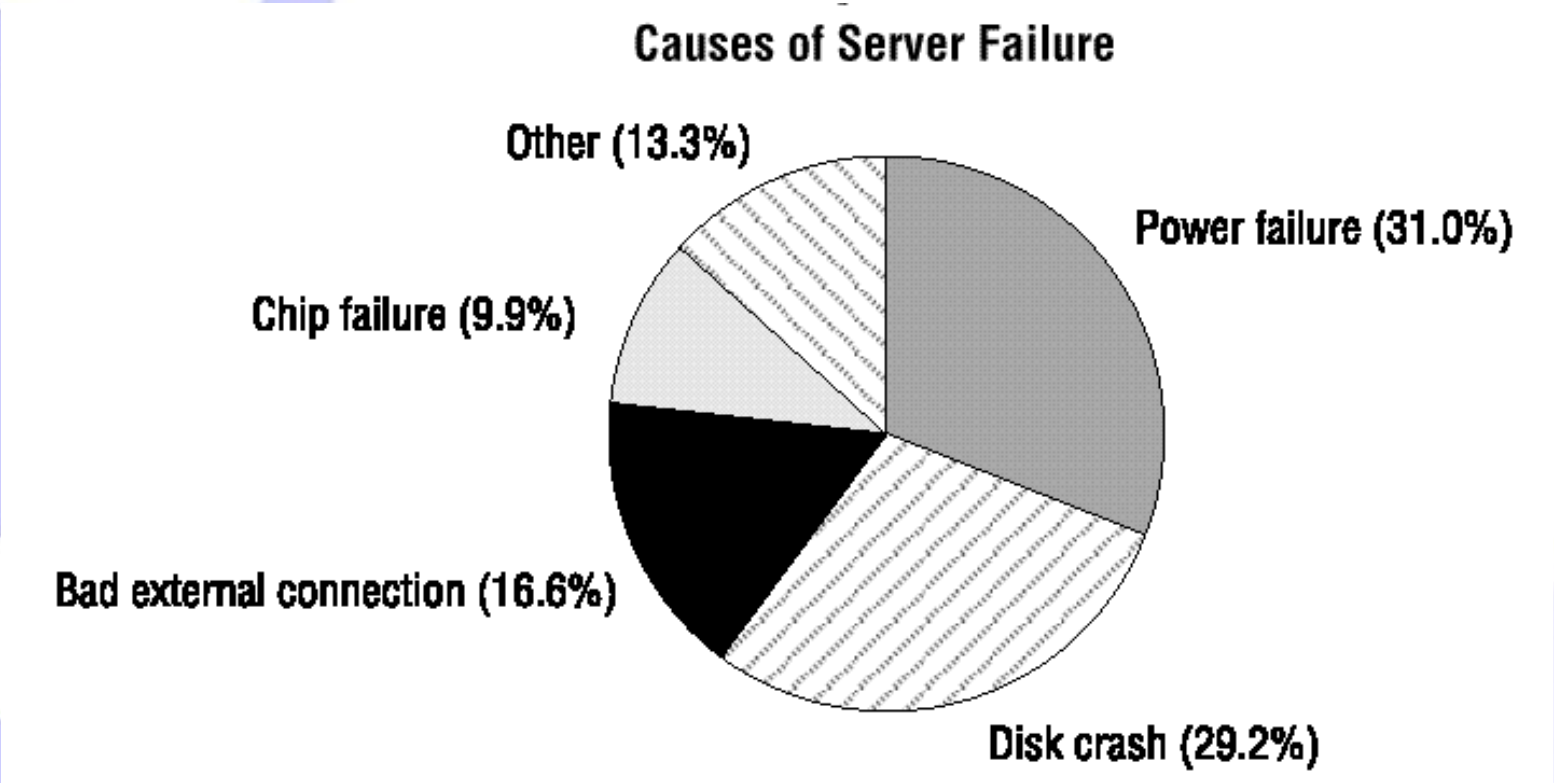
Source: Hewlett Packard Whitepaper, Oct 2008

Economic Costs of Downtime



Source: APC - 1776 Inc.

Power is #1 Cause of Downtime



Source: IDC's Technology Integration Panel Study

Topics

- General Background
- Business Continuity Management
- Management Perspectives
- Caveats

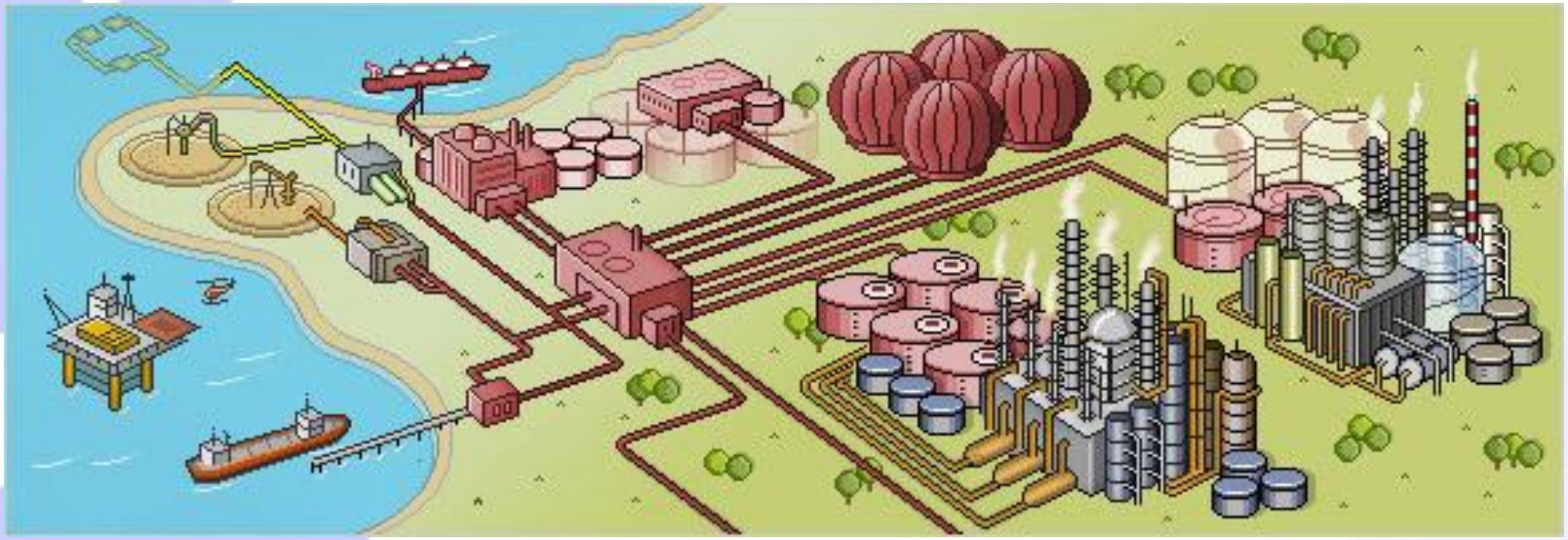
Typical View of Processing Streams in Oil & Gas

Upstream Processes

- Exploration & Appraisal
- Contract Management
- Liquid and Gas Production
- Allocation and Settlement

Midstream Processes

- Bulk Supply Chain Planning and Optimization
- Bulk Supply Chain Operations and Scheduling
- Bulk Supply Chain Execution and Settlement
- Bulk Supply Chain Reporting and Analytics
- Physical Oil and Gas Commodity Trading
- Oil and Gas Paper Trading and Risk Management



Downstream Processes

- Marketing Planning and Execution
- Sales Planning & Account Management
- Opportunity to Cash
- Customer Service
- Terminal Management
- Hydrocarbon Products Transportation
- Service Station Fuel Management
- Convenience Retailing

Concerns in the Banking Industry

Scope of Business Continuity Mgmt

- People
- ICT Systems
- Facilities
  - Office space & Equipment
- Processes
  - In House & Outsourced
- Others
  - Vital documents
  - External dependencies

Objectives

- Operations
  - Prompt continuity of critical ops
- Assets
  - Ensure safety & preserve assets
- Credits
  - Minimize credit loss
- Brand
  - Maintain public confidence

Evolution

- From traditional mainframe DRP/DRC
- Through crisis management planning and BCP
- To the more expansive concept of BCM

Key Elements of BCM

- Understand business environment
- Determine key business parts
- Quantify disruptive impacts
- Identify key resources, infrastructure & tasks
- Establish processes to ensure information updates
- Ensure corporate-wide awareness

Difference Between Risk Management and Crisis Management

Description	Risk Management	Crisis Management
Key Method	Risk Analysis	Business Impact Analysis
Key Parameters	Impact & Probability	Impact & Time
Type of Incident	All types of events	Events causing significant business disruptions
Size of Events	All sizes/costs of events	For strategy planning: Survival threatening incidents only
Scope	Primarily on risks to core-businesses	Mostly outside core-competencies
Intensity	All from gradual to sudden	Sudden or rapid events, though also appropriate for “smoldering” cases

Risk and Vulnerability Assessment

What it is:

- Analysis of threat events and their potential impact on an enterprise's business processes

Objectives:

- Identify key threat events which could cause disruption of services
- Estimate potential of disruption occurring
- Determine client's vulnerability to threat event
- Estimate impact of occurrence of threat event on client
- Evaluate existing threat/risk mitigation measures
- Recommend new/additional threat/risk mitigation measures

Approach:

- Interviews, onsite observations, geographic research
- Assign threat rating for threat events
- Map threat ratings to threat grid

Areas of coverage:

- Natural, human, and technological threats

Deliverable:

- Threat analysis report to include:
  - Analysis of potential threats to business
  - Estimate of financial and operational impact of disruption on business
  - Recommendations to enhance existing/implement new risk prevention/reduction measures

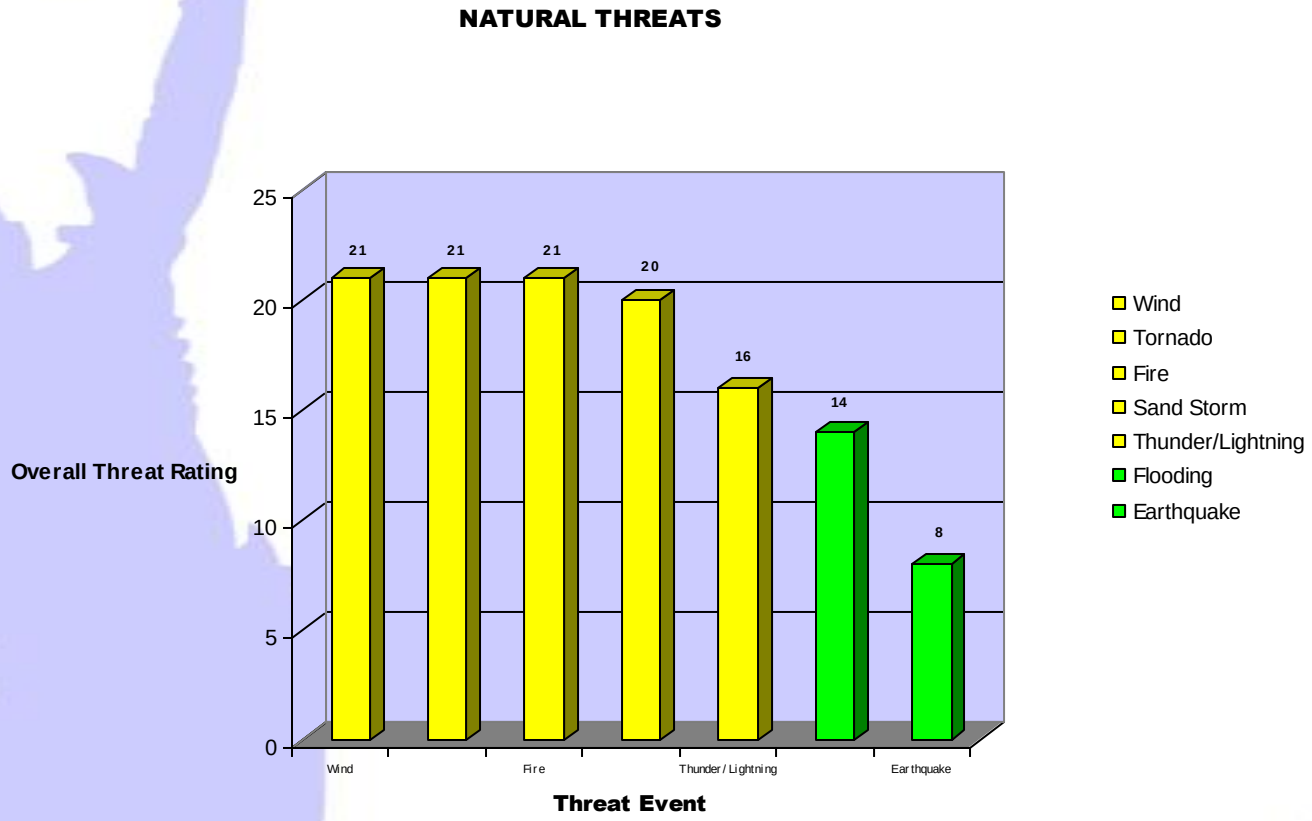
Threat Assessment Scoring

	IMPACT on BUSINESS RATING			SCORING	COMMENTS [1]
XXX <SUBSIDIARY> – Main Office	Impact [2]	Vulnerability	Probability	Overall Score	
	(Impact + Vulnerability) x Probability				
Man-Made Threats (con't)					
Arson	**5**	**2**	**2**	14	**Good fire detection and suppression controls in the corporate data center and the building**
Terrorism / Biological or otherwise	**5**	**3**	**1**	8	Any controls over mail implemented as part of post-09/11?
Nuclear Incident	**5**	**3**	**1**	15	**3 active nuclear plants located within 100 miles of 5500**
Inadequate Training	**4**	**3**	**3**	21	Training programs? X-training?
Computer Virus	**5**	**2**	**4**	28	**Server-based anti-virus software with daily signature file updates; e-mail attachments scanned; firewall blocks inbound .exe files**
Hackers	**4**	**2**	**4**	24	IDS? RAS? Limited dial-up?
Data Entry Errors / Omissions	**3**	**2**	**3**	15	**Impact would depend on the system(s)**
Unauthorized Physical Access	**4**	**4**	**3**	24	**For details, see Physical Security Review (May 2002)**
Malicious Damage or Destruction of Critical Data	**3**	**2**	**3**	15	**The potential of internal threats is substantially greater than the potential for outside malicious damage;** good application controls?

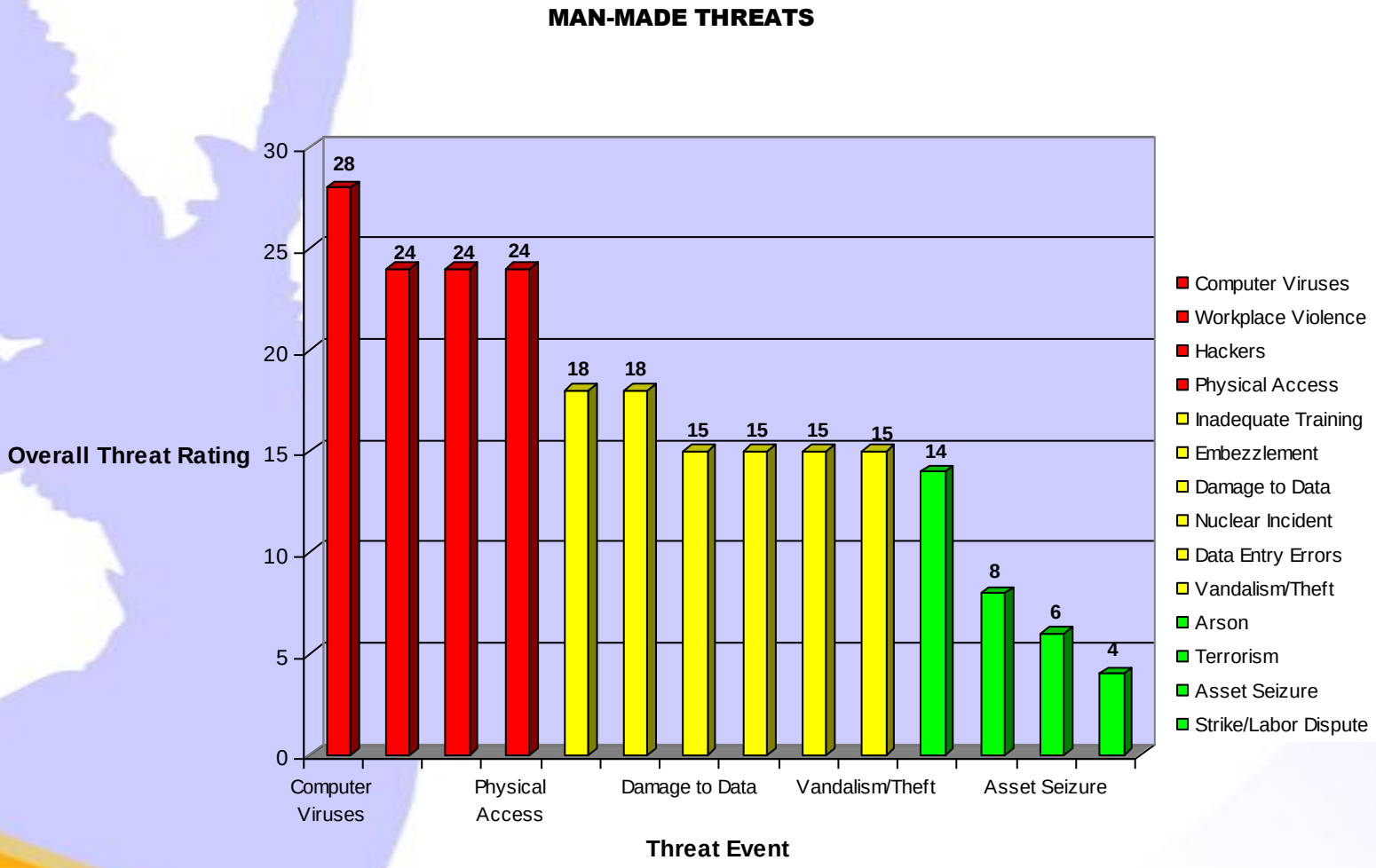
Source data and other considerations taken into account when calculating the vulnerability and/or probability ratings.

Impact ratings: 5 = loss of/access denied to <nnn> building for a prolonged period of time – all critical processes impacted – business can not operate; 4 = loss of /access denied to a substantial part of <nnn> building – some critical processes impacted – major shortfalls; 3 = loss of/access denied to several departments @ <nnn> – a few critical processes impacted – some shortfalls; 2 = loss of/access denied to a few departments @ <nnn> – very little impact on critical processes – a few shortfalls. Where the impact of a threat event could vary (e.g., a fire could destroy the <nnn> building or a localized fire could damage 1-2 departments), we assigned the impact rating based on the worst-case scenario (5) or a partial damage one (3 or 4) based on prior-life experience and historical in-house data.

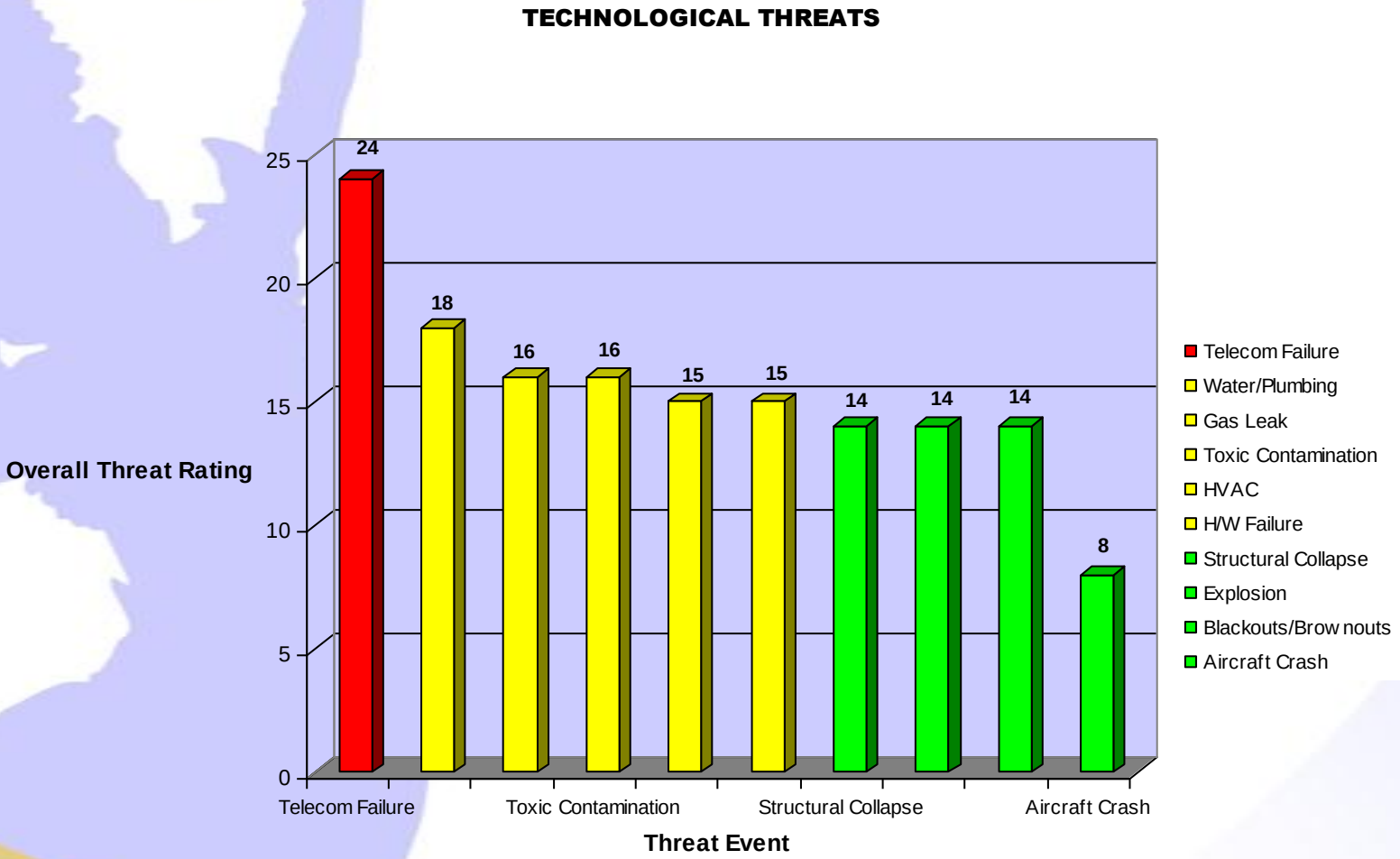
Natural Threats



Man-Made Threats



Technological Threats



Business Impact Analysis (BIA)

What it is:

- Analysis of financial and operational impacts of a disruption on an enterprise's business processes

Objectives:

- Identify critical business processes and associated application systems, IT support services, and internal and external dependencies
- Estimate cost and impact of disruption on critical business processes
- Identify recovery time objectives and acceptable levels of emergency processing
- Identify preliminary recovery resource requirements

Approach:

- Facilitated or individual sessions with business function owners

Deliverable:

- Business impact analysis report to include:
  - Inventory of critical business processes
  - Estimated tangible and intangible impact of a disruption on critical business processes
  - Potential operational impacts of a disruption on critical business processes
  - Minimum time required for each critical business process to recover to an acceptable emergency operating level following disruption
  - Preliminary recovery resource requirements

BIA Working Groups - Setup

Business Impact Assessment needs to be driven from the business side

Business operations have interdependencies that must be identified

Establishing a working group of business owners provides the opportunity to:

- Identify interdependencies between business operations
- Define more realistic impacts due to an interruption to normal operations
  - Tangible impacts
    - Revenue losses
    - Fines, penalties associated with non-performance or service level agreements
    - Contractual obligations
  - Intangible impacts
    - Public image
    - Diminished client service
    - Worker morale
- Identify points of weakness in current operations/procedures
  - Develop steps to eliminate weak points
- Identify points of strength in current operations/procedures that could enable recovery capabilities

Working groups help to minimize time required from business owners to be away from their primary job responsibilities

BIA Working Group - Execution

Facilitated Session(s)

- Facilitator and Documentation Analyst
- Facilitator is a subject matter expert and leads the BIA Working Group in discussion
- White board and easels are utilized to document group discussion as it happens
- Documentation Analyst “captures” all discussions and develops BIA report
- BIA report is distributed to BIA Working Group members for their review
- Facilitator works with BIA Working Group to review and finalize BIA report

BIA Template Completion

- BIA templates are customized to client environment
- Business Owners are identified to participate in the completion of the BIA Templates
- Training session is conducted with all participants
  - Objective of BIA is explained
  - Purpose of participant involvement is explained
  - A case study is used as an example for the completion of the BIA Template
- Business Owners are then required to complete BIA Template on their own
- Subject Matter Experts meet with Business Owners to check on progress and answer questions
- BIA Templates are turned to SMEs who consolidate and create BIA report

BIA – Tangible Impacts

Department	Cumulative Impact 000's						Modules Associated with Department Operations
	Hours		Business Days				
	4	8	2	5	10	30	
Purchasing and Materials Mgt.	0	0	100	525	1000	10000	INV, MDM, PUR, SAL
Production and Manufacturing	0	100	400	400	1000	2000	ACP, ACR, API, BIL, CIM, CST, ORD, DRP, INV, JIT, GLD, MDM, MRP, PUR, SFC, SAL
Order Entry	0	50	400	700	2000	10000	ACR, BIL, ORD, DRP, INV, PRO, SAL
Regulatory	0	0	25	25	50	300	ORD, INV
Metal Carboxylates	100	200	450	850	1000	3000	ACR, BIL, CDM, CST, ORD, INV, CUR, COM, SAL, SAM

BIA - Intangible Impacts

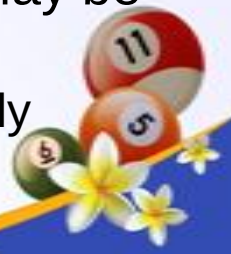
Department	Cumulative Impact Over Time						
	Hours	Business Days					
	4	8	2	5	10	30	Impact Realized
Production and Manufacturing **Customer Service**	**Minimal**	**Moderate**	**Moderate**	**Moderate Heavy**	**Heavy**	**Severe**	Essential 2 Business Days
Goodwill	**None**	**None**	**Minimal**	**Minimal**	**Moderate**	**Moderate Heavy**	
Order Entry **Customer Service**	**Minimal**	**Moderate**	**Moderate**	**Moderate Heavy**	**Heavy**	**Severe**	Essential 2 Business Days
Goodwill	**None**	**None**	**Minimal**	**Minimal**	**Moderate**	**Moderate Heavy**	
Regulatory **Customer Service**	**None**	**None**	**Minimal**	**Minimal**	**Moderate**	**Moderate Heavy**	Important 5 Business Days
Goodwill	**None**	**None**	**None**	**Minimal**	**Minimal**	**Moderate**	
Metal Carboxylates **Customer Service**	**Minimal**	**Moderate**	**Heavy**	**Severe**	**Severe**	**Severe**	Vital 4 Hours
Goodwill	**Minimal**	**Moderate Heavy**	**Severe**	**Severe**	**Severe**	**Severe**	

Topics

- General Background
- Business Continuity Management
- Management Perspectives
- Caveats

Corporate Objectives:
Some Examples

- Market impact and influence on investor perceptions, or in other words: how will BCM stimulate share price for publicly listed companies
  - Usually a reactive response since local investors tend not to directly appreciate BCM
  - But impact may be “disastrous” (especially foreign investors and owners) when disaster strikes and the company can not manage business continuity well
- Customer impact when perception is depleted due to bad business continuity
  - In an extreme situation: a corporate failure where the plant (or even the entire company) may fail to continue operations
  - More often: perception of a company being “bad” due to low quality recovery
- Regulatory impact related to compliance factors, which in turn may be risk-driven
  - Regulations (including reporting) and compliance thereto will directly impact a company’s “health”
  - Evaluation results in this category tend not to be publicly known



Managing Implementation

- Wherever and whenever affordable:
  - Keep away from crisis risk-taking
  - Keep the risk-taking away from the business
- This can be done by:
  - Rely on experts and dependable systems
  - Ensure the bidding and acquisition process really provides the best solution and not just the cheapest solution

Topics

- General Background
- Business Continuity Management
- Management Perspectives
- Caveats

Caveats

- Proper Crisis Management and BCM do not necessarily always make a company “good”
  - A lot will still depend on other management and operational aspects
  - Relevant external factors will continue to influence
- “No plan ever survives first contact with the enemy”
  Von Clausewitz (1780-1831): “On War”
  - No amount of planning will ever allow us to fully predict the nature of a (first-time) crisis
- The “best preparation” is:
  - A robust, quick, flexible and *practised* response structure that can adapt to different circumstances
  - Broad representation of senior management and critical support departments in making decisions
  - A clear and well documented decision-making & authorization process
  - Good, open communications in every direction

Crisis Management:
A Senior Executive Perspective

Thank You