AFP®
Association for Financial Professionals®
AFP Annual Conference
ORIGINAL ESSENTIAL UNBIASED INFORMATION

Business Continuity: Pondering the Unponderable

A Corporate-Bank Dialogue on Planning, Prevention and Protagonism

AFP®
Annual Conference

Association for Financial Professionals®

ORIGINAL ESSENTIAL UNBIASED INFORMATION

Jim Loewen, CTP
Assistant Treasurer
Consumers Energy

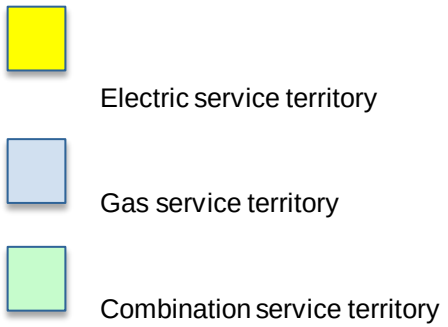
- 30+ Years experience in TM and cash operations
- Treasury lead in company wide development and implementation of BC/DR plan

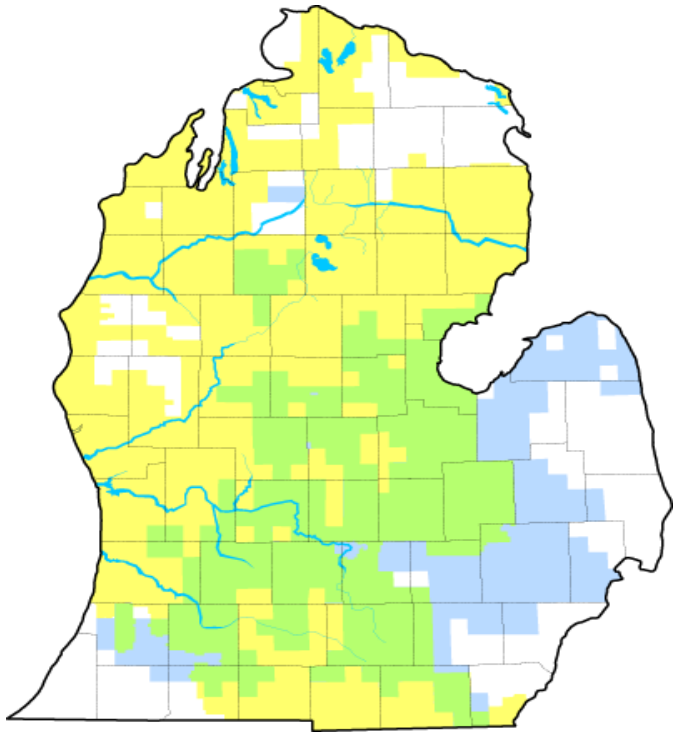
Dan McCarty
SVP – TM Market Manager
PNC Bank

- 30+ Years experience in commercial lending and treasury managementM
- Member and past Chair: ABA Payment Systems Committee

Consumers Energy

- Fourth largest combination utility in the U.S.
- 1.8 million electric and 1.7 million gas customers
- 7,700 employees
- $6.3 billion revenue
- $15.7 billion assets





PNC Bank Corporate Profile

Employees:
Approximately 57,000 in the U.S. and abroad

Size by Deposits:
6th largest U.S. bank by deposits

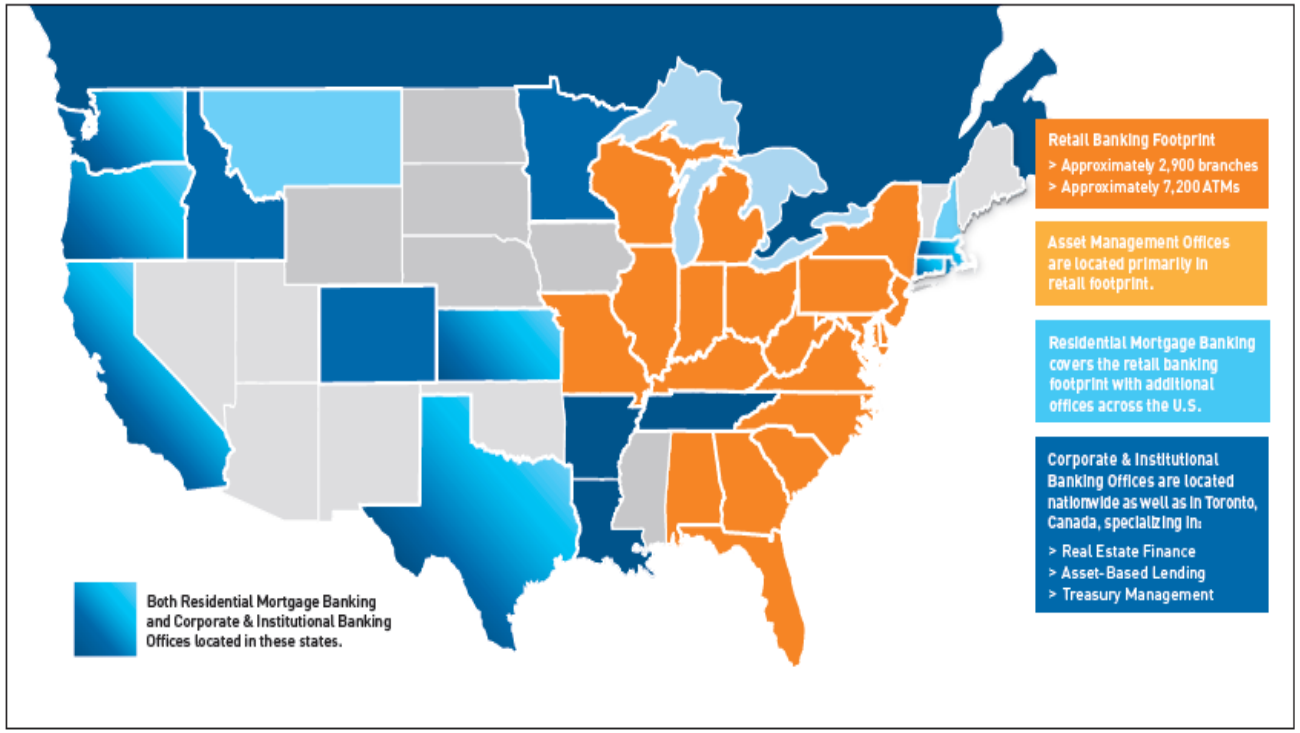
Customers:
More than 6 million consumer and small business customers

Locations:
Branches - About 2,900 in 18 states and the District of Columbia

Brokerage Offices - 40 offices in 12 states and the District of Columbia

ATMs:
More than 7,200 machines

Internet Address:
www.pnc.com



Pro Forma Financial Highlights*	
Assets	$296 billion
Deposits	$206 billion
Shareholder Equity	$35 billion
*As reported 03/31/12	

Ideas for our Discussion

- Concerns of Sub Optimal BC/DR: Risk Factors
- Real Life: Some Examples to Consider
- Business Continuity/Disaster Recovery… …What's Involved
- Focus of Contingency Planning: Corporate-Bank Interactions
- Ideas for Your Consideration

Ideas for our Discussion

- Concerns of Sub Optimal BC/DR: Risk Factors
- Real Life: Some Examples to Consider
- Business Continuity/Disaster Recovery… …What's Involved
- Focus of Contingency Planning: Corporate-Bank Interactions
- Ideas for Your Consideration


Operational
Credit
Market
Corporate Risk
Regulatory
Reputation
Environmental

Risk of An Ineffective BC/DR Plan

- **Disrupt network operations; cause business to come to a halt**
- **Reduction of Business Revenues**
- **Continuance of Expenses**

- **Impact on Corporate Brand: Incalculable**

Risk of An Ineffective BC/DR Plan

- **Potential of Costly Litigation**
- **Impact on Future Operations**
- **Potential Loss of Clients**

- **Worst case scenario: Business Closure**

Top Threats to Business Continuity

Business Continuity Institute

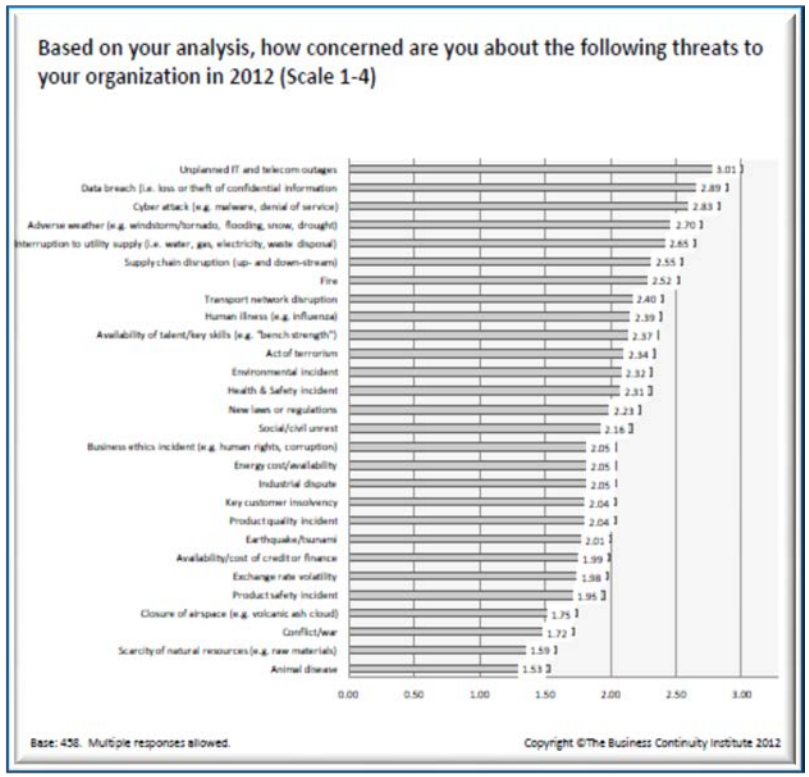
In this chart, each threat is evaluated against scale which translates into a score as follows:

- Extremely Concerned: 4
- Concerned: 3
- Somewhat concerned: 2
- Not concerned: 1

Note: *not applicable* is available as a non-scoring choice.

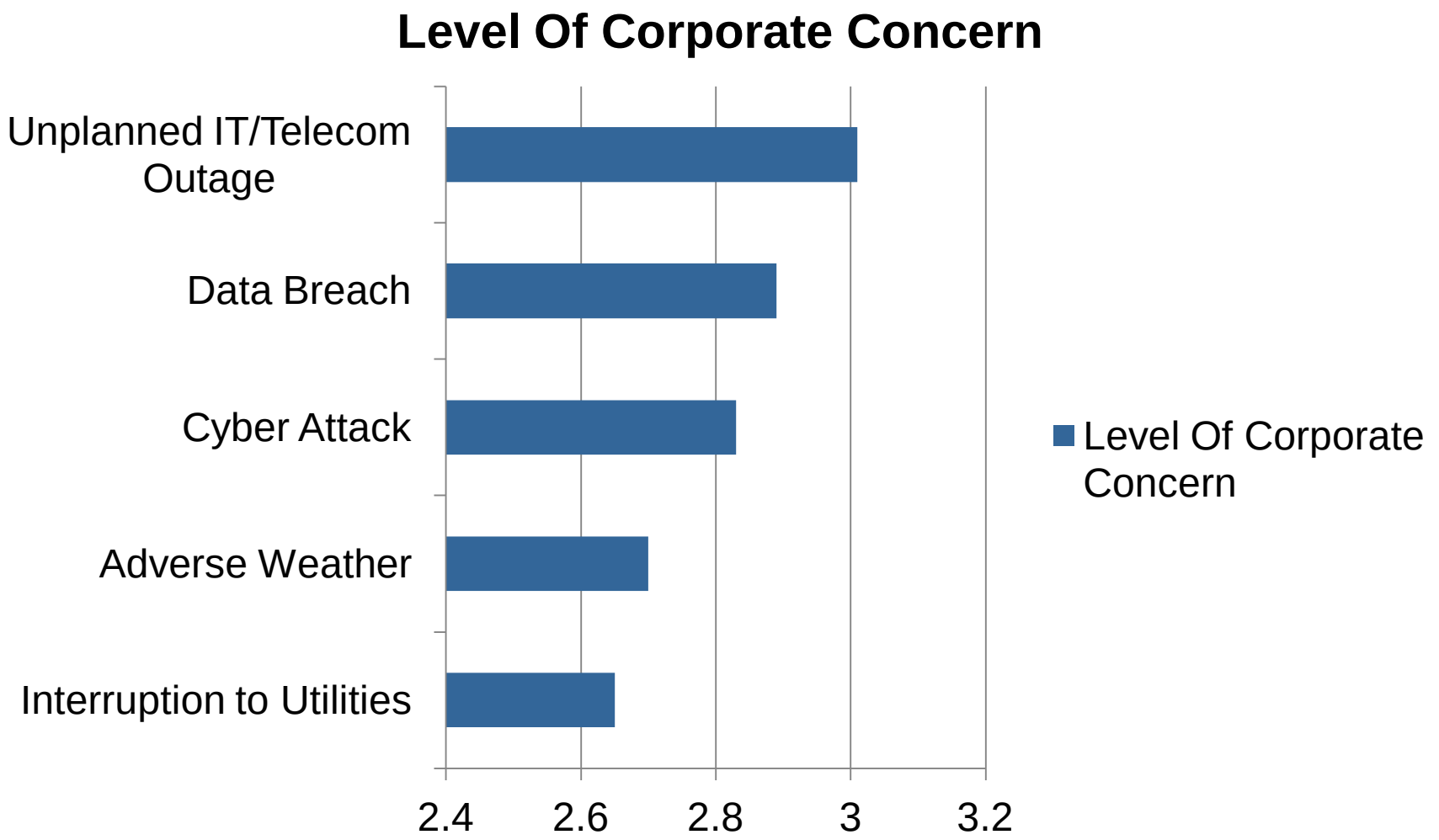
The highest score would be 4.00 which would equate to 100% of respondents for whom the threat is applicable marking it as *extremely concerned*.

This approach has generated some differences further down the scale where *somewhat concerned* numbers are a significant proportion. For example, *human illness* scores 2.39 or 9th position under this scoring method rather than 17th.

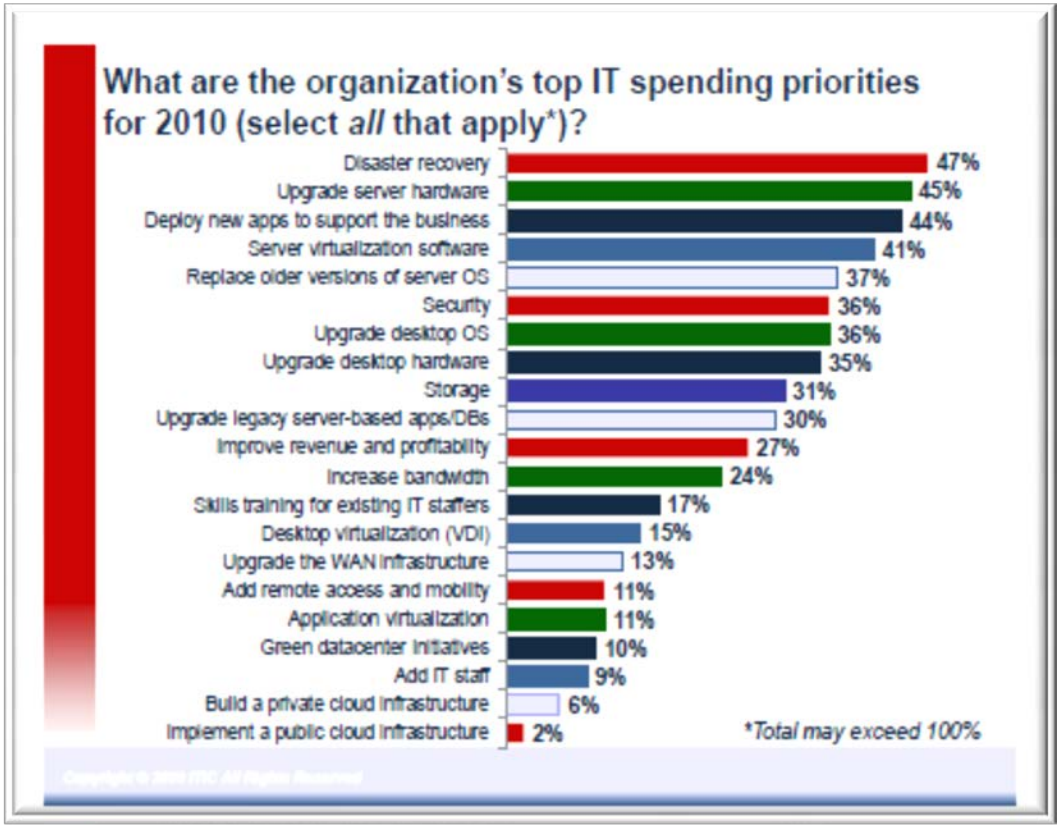


See Appendix A

Top Threats to Business Continuity



Follow the Corporate Investment



The flow of investment for IT Spend appears to match the concerns related to Business Continuity!

See Appendix B: College of Virtualization: Lessons in Implementing a Cost-Effective Disaster Recovery Plan Sponsored By: Dell & VMware

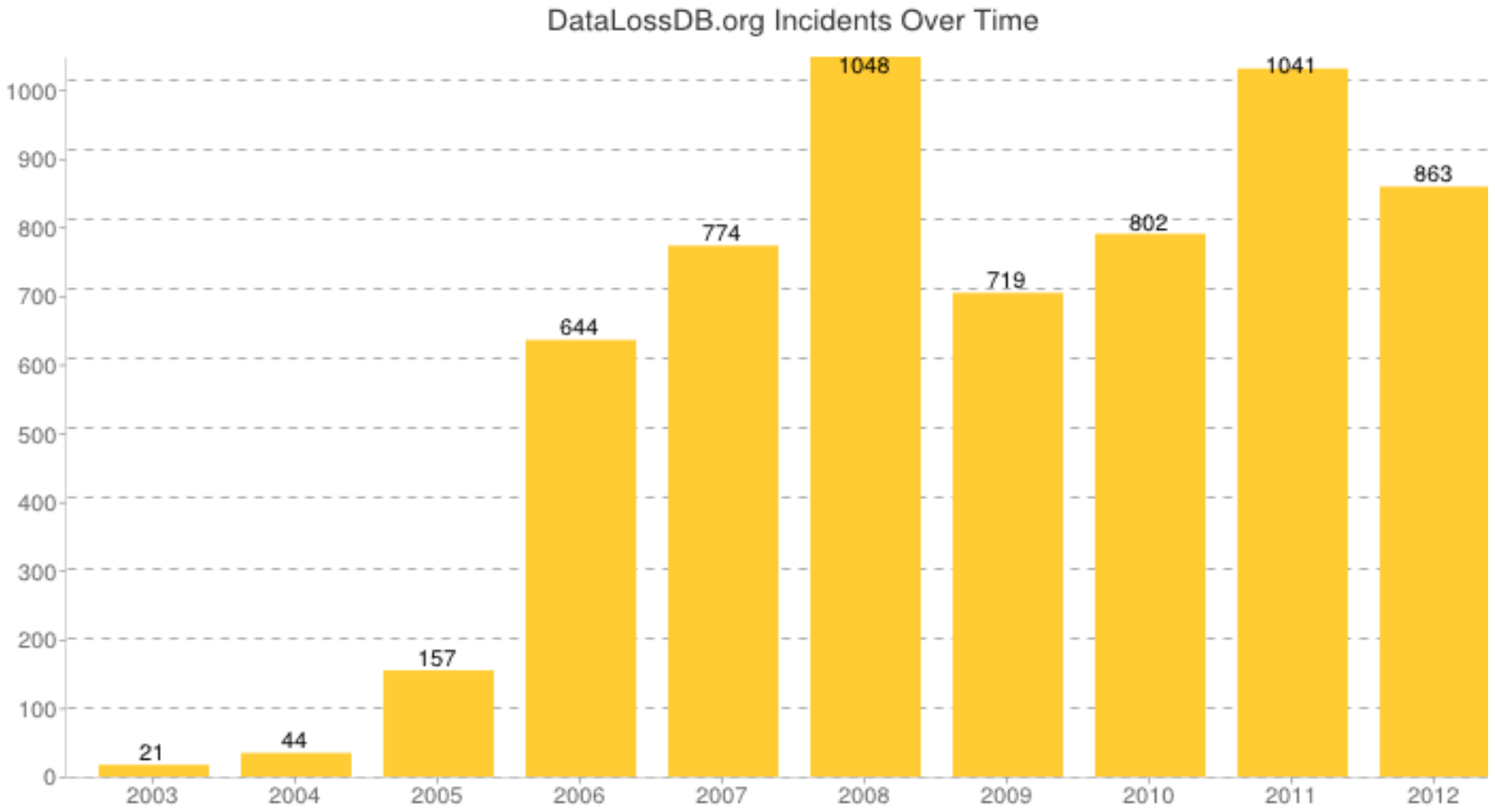
Ideas for our Discussion

- Concerns of Sub Optimal BC/DR: Risk Factors
- Real Life: Some Examples to Consider
- Business Continuity/Disaster Recovery… …What's Involved
- Focus of Contingency Planning: Corporate-Bank Interactions
- Ideas for Your Consideration

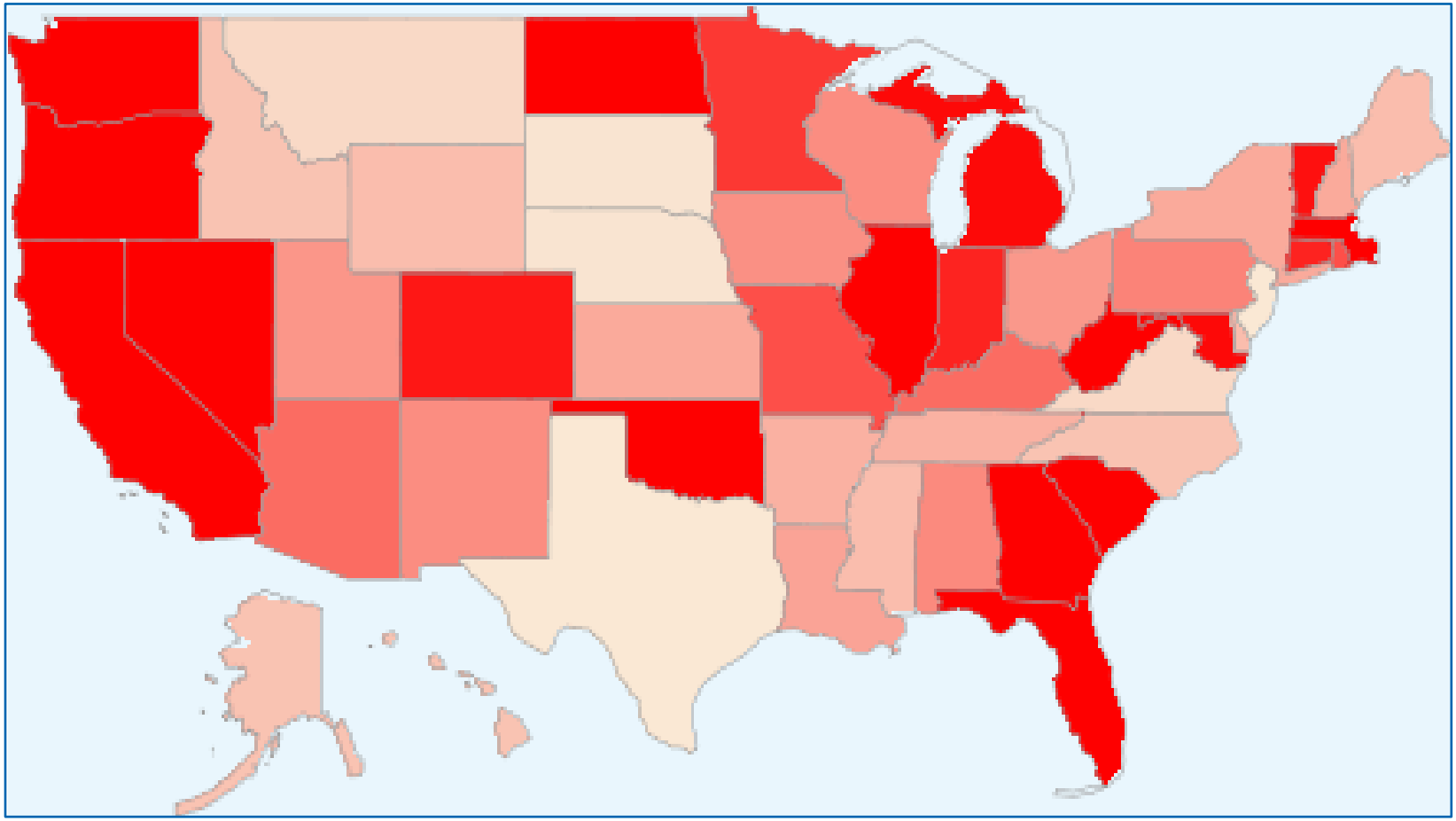
Disruptive Events… Some Examples

- **September 11th, 2001**
  - Too Many to Mention
- **August 14th, 2003**
  - Power Outage: August 14, 2003 at 4:10pm ET
- **August 23rd-30th, 2005**
  - Hurricane Katrina and Hibernia Bank
- **May, 2010**
  - Downtown Nashville Flood
- **February, 2011**
- **Every other day**
  - Data Breaches: TJX, Heartland, Sony…Global Payments

Disruptive Events… A Time Line



Disruptive Events… By Location



Disruptive Events… Data Breaches

Ideas for our Discussion

- Concerns of Sub Optimal BC/DR: Risk Factors
- Real Life: Some Examples to Consider
- Business Continuity/Disaster Recovery… …What's Involved
- Focus of Contingency Planning: Corporate-Bank Interactions
- Ideas for Your Consideration

What's Involved

- **Business Continuity vs. Disaster Recovery**
  - **Differentiate**
- Focus: What are you trying to accomplish
  - RTO v. RPO: Have an SLA
- Business Continuity: A Process
- Impact Analysis: a Questionnaire
  - See Appendix C
- Business Continuity: a Corporate Example

Consumers Energy: Definitions

- **Crisis Management**
  - The infrastructure needed to manage disasters
- **Business Continuity**
  - The advance arrangements for continuing critical business processes if the primary work location and/or primary applications are unavailable
- **Disaster Recovery**
  - A plan to recover those critical IT systems or infrastructure necessary to support key business processes in the event of a disaster

Crisis Management Plan (Yellow)

What's Involved

- Business Continuity vs. Disaster Recovery
  - Differentiate
- **Focus: What are you trying to accomplish**
  - **RTO v. RPO: Have an SLA**
- Business Continuity: A Process
- Impact Analysis: a Questionnaire
  - See Appendix C
- Business Continuity: a Corporate Example

Focus: What are you trying to accomplish?
Classification of Tasks

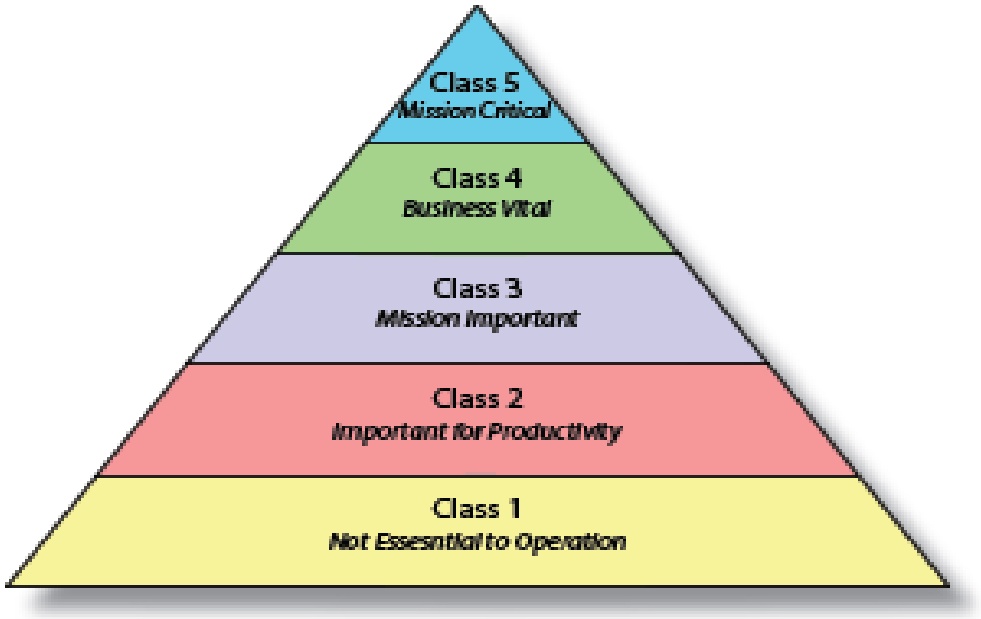
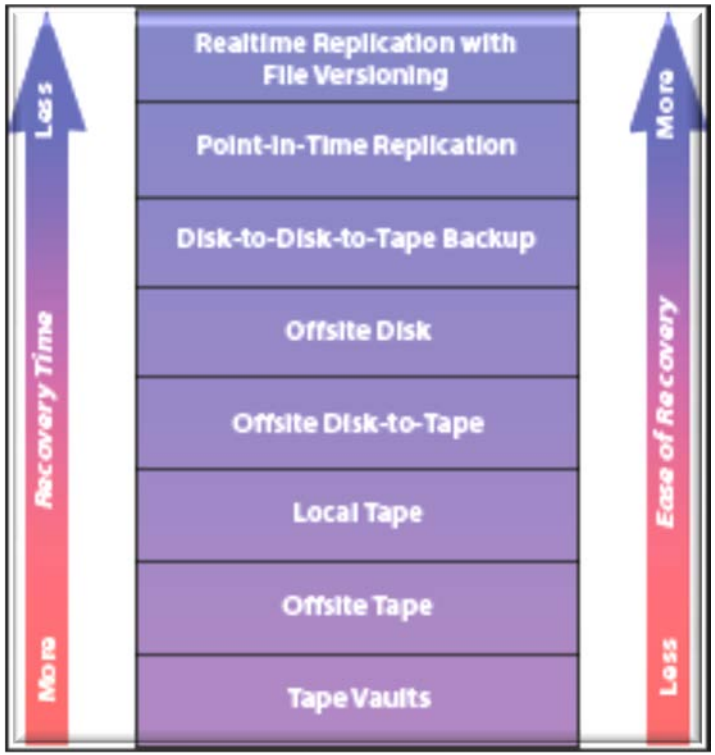


Figure 1: Data Value Hierarchy

Business Continuity: RTO vs. RPO

Have an SLA for your Recovery Time Objective…



… and for your Recovery Point Objective Too!!!

What's Involved

- Business Continuity vs. Disaster Recovery
  - Differentiate
- Focus: What are you trying to accomplish
  - RTO v. RPO: Have an SLA
- **Business Continuity: A Process**
- Impact Analysis: a Questionnaire
  - See Appendix C
- Business Continuity: a Corporate Example

Business Continuity: A Process

- Governance
- Program Components
- Strategic Investments and Solutions Development
- Strategic Partnerships
- Industry Trends

Business Continuity: A Process

Program Components

- Analysis and Planning
- Operational Availability
- Testing
- Training and Awareness
- Reporting
- Crisis Management

Business Continuity: A Process

Analysis and Planning

- Understand and quantify business exposures/potential impact
- Plan for the recovery of key resources: people, processes, technology, facilities and vendor/partners
- Transparent reporting for recovery capabilities, residual risk and remediation
- Identify enhancements to Business Continuity Plan: Prioritize!
- Coordinate remediation with investment priorities
- Facilitate risk based decision making
- Develop escalation criteria for an event: great or small

Business Continuity: A Process

Testing

- Validate recovery strategies at least annually or as necessary
- Review results with business unit, management, audit and regulatory agencies
- Gaps and enhancements tracked and prioritized for funding and completion
- Technology tests conducted at least annually
  - Assuming primary data centers are unavailable
  - Use of real time information
  - Involve entire chain of distributed systems

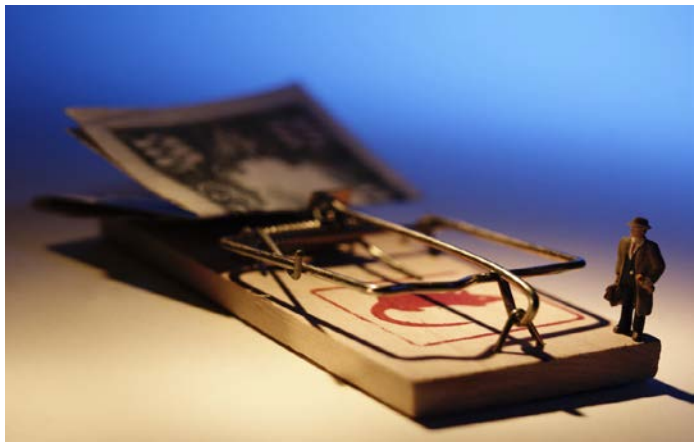
Reporting

- Integrated into BRP: Summarize and highlight recovery/ business resumption across business lines
- Provide transparent overview across all dependent units and to all levels of management

Business Continuity: A Process

Crisis Management

- Crisis management teams:
  - Impact assessment
  - Notification of appropriate parties
  - Escalation to management
  - Coordinate overall effort
- Crisis communication: Regular updates with impact assessments to affected parties: Customers, employees, vendors, regulators
- Scenario based walkthroughs:
  - Understanding of crisis response
  - Impact assessment
  - Resumption capabilities
- Testing



Consumers Energy: A Bit of History

- **2009 Internal Audit report**
  - Incomplete or nonexistent business continuity plans
  - No business continuity training
  - No comprehensive policy
- **2010 Project**
  - Development and implementation of policy, oversight structure and plans

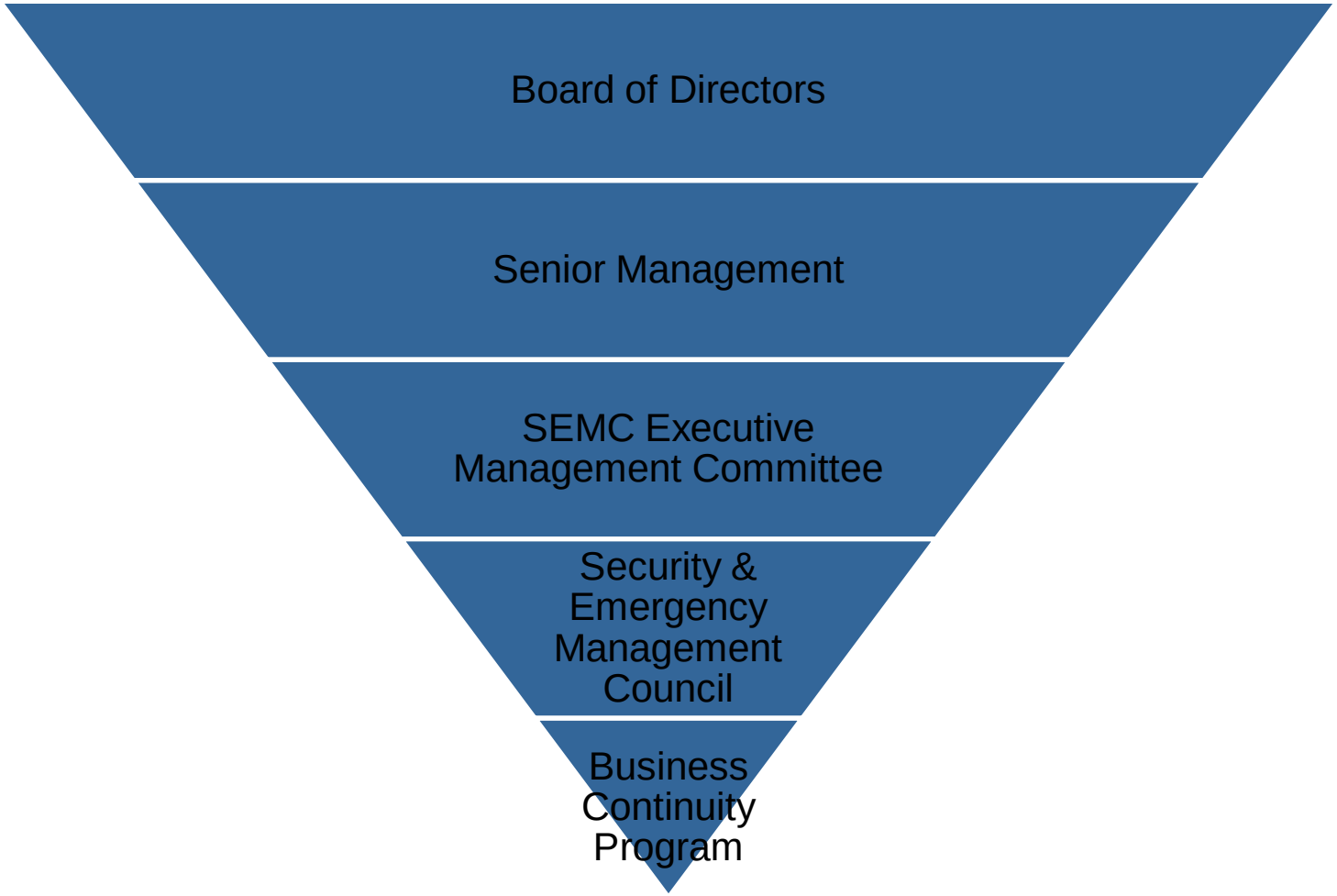
What's Involved

- Business Continuity vs. Disaster Recovery
  - Differentiate
- Focus: What are you trying to accomplish
  - RTO v. RPO: Have an SLA
- Business Continuity: A Process
- **Impact Analysis: a Questionnaire**
  - **See Appendix C**
- Business Resiliency: a Corporate Example

What's Involved

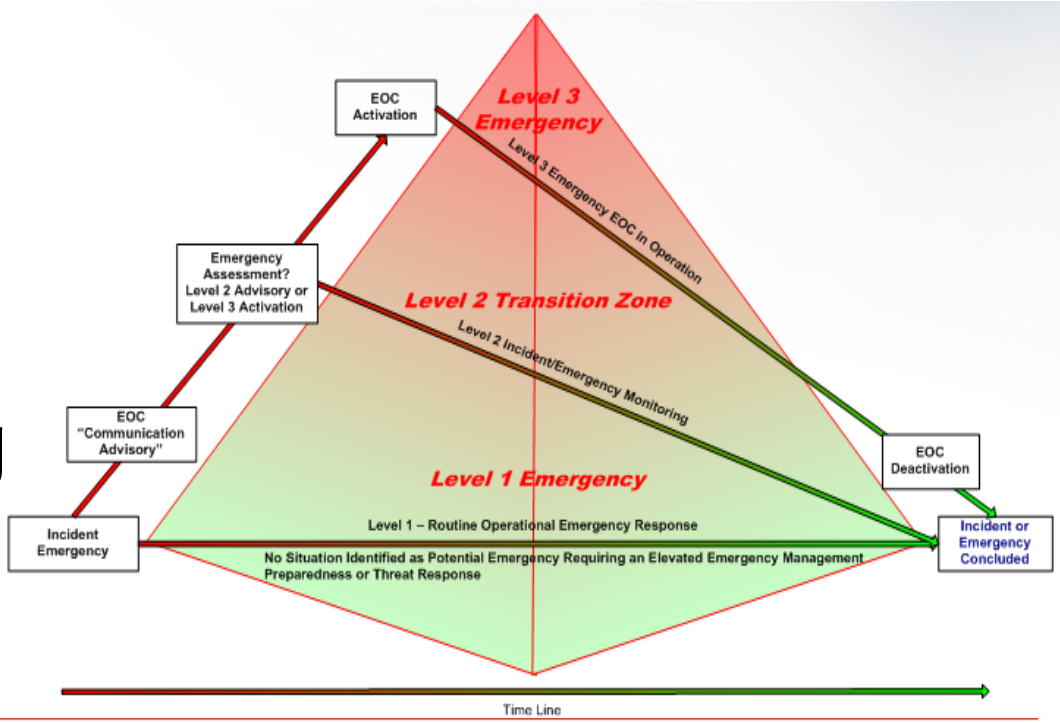
- Business Continuity vs. Disaster Recovery
  - Differentiate
- Focus: What are you trying to accomplish
  - RTO v. RPO: Have an SLA
- Business Continuity: A Process
- Impact Analysis: a Questionnaire
  - See Appendix C
- **Business Continuity: a Corporate Example**

Consumers Energy: Governance

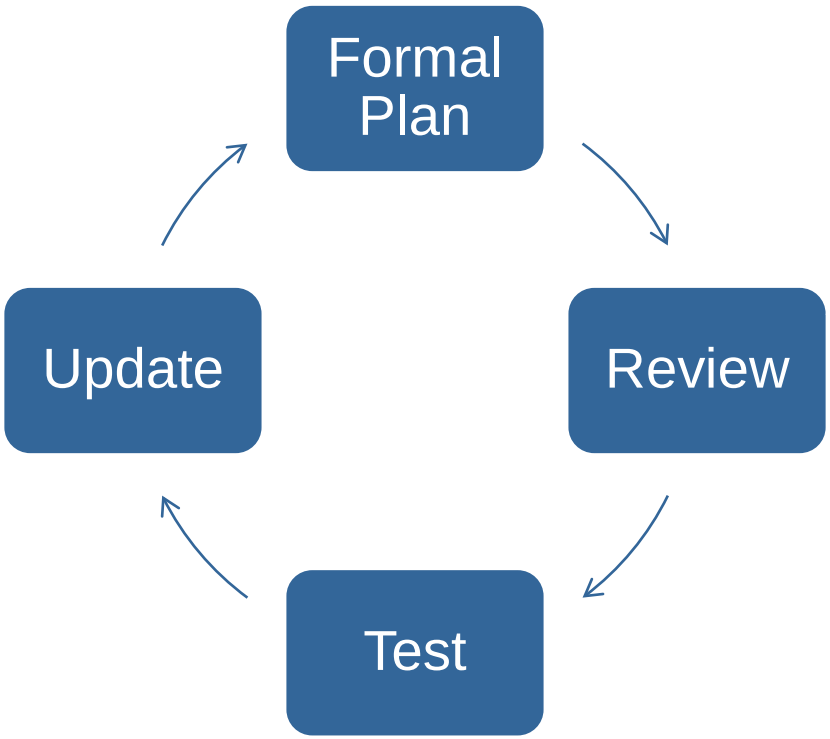


Consumers Energy:
Emergency Operations Center

- **Emergency Management**
  - Incident Command
- **Key Personnel**
- **Annual Testing**



Consumers Energy: Business Continuity Cycle



Consumers Energy: Technology

- **Business Impact Analysis**
  - Priority Application Listing
  - Company-wide prioritization of all systems and applications
- **Treasury**
  - Bank account database
  - Contacts database

Consumers Energy: Treasury's Plan

- **Work at Home**
  - Laptops
- **Access to Key Contacts**
- **Bank Account Database**
- **Bank Reporting and Transaction Initiation Systems**
- **48 Hour Maximum Interruption**

Ideas for our Discussion

- Concerns of Sub Optimal BC/DR: Risk Factors
- Real Life: Some Examples to Consider
- Business Continuity/Disaster Recovery… …What's Involved
- Focus of Contingency Planning: Corporate-Bank Interactions
- Ideas for Your Consideration

Financial Planning: Contingencies

Collections

- **Lockbox:**
  - Can you receive data for posting?
  - Exception management: Post cash and correct issues later?
- **Wires (inbound):**
  - Do you have event notification?
  - Information reporting: Intraday?
  - Related data: FED reference number; Expanded remittance
- **ACH (inbound):**
  - Do you have event notification?
  - Information reporting: Intraday?
  - Related remittance data: CTX; CCD+
- **Card:**
  - Notification
  - Level 1-3 data: Can you receive it for posting?

Financial Planning: Contingencies

Disbursements

- **Demand Accounts (Checking):**
  - Authorized signers/resolutions: Limits, number of signers, physical location: Do you have paper and electronic copies?
  - Check stock: Accessible?
  - Check Positive Pay implications: Pay or no pay?
  - Card access to account?
- **Wire:**
  - Voice wires: Do you have PIN process established?
  - Branch origination: Hours of operation; dollar limits; PINs
  - Deadline of FED wire system
- **ACH:**
  - Can you create/confirm a payment/file (system availability)
  - Windows of operation: ACH network and your bank
  - Dual approval: Access and availability
  - ACH Positive Pay implications

Financial Planning: Contingencies

Information Reporting

- Visibility of activity (and of Cash!)
- Accessibility to company systems, web and bank systems

Liquidity

- Daylight OD limits: For your company? For your bank?
- Availability of cash when receipts are interrupted
- Overdraft (overnight) vs. extension of credit

Communications – Immediate and Ongoing

- Management and staff (Communication Tree)
- Key customers
- Vendor/Suppliers: Banks, third party service providers
- Insurance providers: notification may provide resources

Facility Planning

- Primary and secondary operating sites
- Securing your facility and related assets (sanitation, water etc.)
- Supplies unique to your business

Ideas for our Discussion

- Concerns of Sub Optimal BC/DR: Risk Factors
- Real Life: Some Examples to Consider
- Business Continuity/Disaster Recovery… …What's Involved
- Focus of Contingency Planning: Corporate-Bank Interactions
- Ideas for Your Consideration

Ideas for Consideration

Implement Electronic Processes Wherever Possible

- Improve recovery options
- Planned redundancy
- Remote accessibility
- Increased communication alternatives
- Security and system integrity

Collections

- Plan for data interruption on both sides: Corporate and bank
- Decisioning for cash application separate from A/R data
- Have distribution plans for data
  - Alternate addresses for paper and electronic delivery

Disbursements

- Consider methods for payment origination
  - ACH to wire? Electronic to paper?
- Plan now for alternate approval process
- Consider commercial cards for appropriate payments

Ideas for Consideration

Payment System Redundancy

- Internet access
- Maintain security within an event
- Monitor activities during an event
- Commercial cards

Status and Location of Account Information

- Do you have backup copies of information?
- Do you have sufficient cash available for initial needs?

Develop a List of Priority Payment Activities

- Payroll
- Key supplies
- Utilities

Talk to your bank…NOW!!!!

AFP®
Annual Conference

Association for Financial Professionals®

ORIGINAL ESSENTIAL UNBIASED INFORMATION

Thank You!!!!!!

Standard Disclosure

- **PNC, PINACLE, Working Cash, ActivePay, Global Trade Excellence, XPACK and Vested Interest are registered marks of The PNC Financial Services Group, Inc.("PNC")**
- **Midland Loan Services, Enterprise!, CMBS Investor Insight, Portfolio Investor Insight, Borrower Insight, Deal Flow and Shared Servicing are registered marks of PNC Bank, National Association.**
- **Banking and lending products and services and bank deposit products and investment and wealth management and fiduciary services are provided by PNC Bank, National Association, a wholly-owned subsidiary of PNC and Member FDIC. Certain fiduciary and agency services are provided by PNC Delaware Trust Company. Equipment financing and leasing products are provided by PNC Equipment Finance, LLC, a wholly-owned subsidiary of PNC Bank, National Association. Aircraft financing is provided by PNC Aviation Finance, a division of PNC Equipment Finance, LLC. Merchant services are provided by PNC Merchant Services Company. Private equity financing is provided by affiliates of PNC Equity Management Corp. Mezzanine financing is provided by PNC Mezzanine Capital Corp. Investment banking and capital markets activities are conducted by PNC through its subsidiaries PNC Bank, National Association, PNC Capital Markets LLC, and Harris Williams LLC. Services such as public finance advisory services, securities underwriting, and securities sales and trading are provided by PNC Capital Markets LLC. Merger and acquisition advisory and related services are provided by Harris Williams LLC. PNC Capital Markets LLC and Harris Williams LLC are registered broker-dealers and members of FINRA and SIPC. Harris Williams & Co. is the trade name under which Harris Williams LLC conducts its business. Foreign exchange and derivative products are obligations of PNC Bank, National Association. Securities products and brokerage services are offered through PNC Investments LLC, a registered broker-dealer and member of FINRA and SIPC. Insurance products and advice may be provided by PNC Insurance Services, LLC.**
- **Important Investor Information: Brokerage and insurance products are:**
  - Not FDIC Insured. Not Bank Guaranteed. May Lose Value.
  - PNC does not provide legal, tax or accounting advice. PNC does not provide investment advice to Vested Interest plan sponsors or participants.
- **Lending and leasing products and services, including card services, trade finance and merchant services, as well as certain other banking products and services, require credit approval.**
-

Sample business impact analysis questionnaire

By Paul Kirvan, FBCI, CBCP, CISA

A business impact analysis (BIA) attempts to relate specific risks and threats to their impact on key issues like business operations, financial performance, reputation, employees and supply chains. The BIA is usually the starting point for risk identification in a business continuity context and the analysis' results should guide the risk assessment process.

The discovery process relies on questionnaires to gather relevant information. The person creating the BIA works to identify business attributes such as critical business processes, interdependencies among business units (both internal and external), supply chain dependencies, minimum acceptable office configurations and supplies, minimum time needed to recover operations, as well as minimum staffing required to provide business as usual. BIA questions are posed to key members of each operating unit in the company. A well-organized BIA questionnaire should be able to fulfill its discovery objectives in no more than 20 to 25 questions.

The template below contains topics for suggested questions in your organization's business impact analysis questionnaire.

SAMPLE QUESTION/TOPIC	NOTES
Business processes	*Describe the business processes for your business unit; minimum acceptable recovery time frames for the business unit, and for specific processes (e.g., accounting), applications (e.g., email), etc.*
Dependencies among business units/processes	*Define the business units and/or processes and/or systems that a business unit/process depends on to perform normally; specify if these are internal or external to the organization, such as supply chains.*
Criticality of business processes	*To the greatest extent possible, determine which business units and/or processes are the most essential to the company and its operations.*
Availability of alternate business processes, staffing and resources	*Specify alternate procedures, e.g., paper work orders or paper order forms, that can be used in lieu of the principal process; access to temporary staffing; and access to alternate operating resources such as a hot disaster recovery site.*
Work backlog	*For each defined business unit and/or process identified, how long will it take (e.g., hours) to process daily backlogs for each day of downtime? What technique is used, e.g., concurrent or sequential processing?*
Critical records	*Specify critical business records by record name,*

	type of media, primary location of records and alternate location (as required).
Reporting requirements	*What specific internal/external reporting, such as for regulatory requirements, is needed? Include the report name, author(s), recipient(s), frequency, delivery requirements, variances allowed and penalties (if any).*
Difficulty of recovery	*Define potential recovery issues in terms of difficulty to recover operations, time needed to recover and resources needed to recover.*
Difficulty of restoration	*Define potential restoration issues in terms of difficulty to restore operations to an as-normal or near-normal state.*
Tolerance to outages	*Assuming a serious situation, such as destruction of the company's headquarters locatio**n,** how long (hours or days) could the business unit and/or system/application be unusable before its loss would impact the organization, its stakeholders, suppliers, regulators, etc.?*
Maximum time for disruption to business functions/processes/systems	*Determine the maximum amount of time, e.g., hours, days, weeks, months, that business units, functions, processes, systems, employees, office space, etc. can be unavailable before the firm loses business, market share, revenues, customers, etc.*
Disruption impact by timeframe	*Using an acceptable time frame, such as days, weeks or months, define the impact to the organization if an event occurs at certain times of the year, or certain days of the month.*
Disruption impact by severity of incident	*Specify the degree of severity of the identified outage or disruption, e.g., worst case = 5, no impact = 0.*
Disruption impact by line of business	*Specify the line of business (e.g., manufacturing, accounting) and the impact to that activity, e.g., worst case = 5, no impact = 0.*
Disruption impact by operation	*Define operational impacts, such as cash flow, competitive position, public image, reputation, staff morale, employee hiring and retention, financial reporting, stakeholder perceptions, shareholder perceptions, and the impact to that activity, e.g., worst case = 5, no impact = 0.*
Financial impact	*Determine the estimated impact to earnings, profits, expenses, etc., in a variety of time frames, such as days, weeks and months.*
Minimum acceptable staffing	*Specify the minimum number of people needed for each business unit to operate as-normal or near-normal.*
Minimum acceptable configuration of systems	*Specify minimum number of physical systems, such as servers, routers, switches, workstations, laptops, phones, copiers to resume limited*

	operations.
Minimum acceptable applications	*Specify minimally necessary operating systems, databases, applications, utilities, etc. needed for employees and operations.*
Minimum acceptable infrastructure requirements	*Specify such items as power, HVAC, voice and data communications, water supplies, food supplies.*
Minimum acceptable space requirements	*Specify minimum physical space required by employees, e.g., 40-50 square feet.*
Minimum acceptable work space requirements	*Specify such items as office supplies, furniture, lighting, phone/data connections, electrical outlets.*
Define unique or specialized requirements	*There may be a need for specialized systems, such as high-speed printers, plotters and graphics workstations; define the minimally acceptable number and type.*
Anticipated changes to the business	*Provide details on special situations, such as mergers and acquisitions and planned physical moves, the presence of which could affect how the organization recovers.*
Other	*Specify any other issues or concerns that may affect the recovery of a business unit, systems supporting that business unit, staffing, etc.*

HORIZON SCAN 2012

BCI Survey Published January 2012

Global business continuity concerns are driven by IT and Internet vulnerabilities in 2012.

Dominating the horizon scanning of business continuity professionals around the world are threats arising from IT, telecom and Internet dependencies.

The top threats evaluated through risk assessment, based on those registering *extremely concerned* and *concerned*, include the following:

- Unplanned IT and telecom outages
- Data breach (i.e. loss or theft of confidential information)
- Cyber attack (e.g. malware, denial of service)

It would be wrong, however, to push these threats down to IT departments to deal with. Data breaches and cyber attacks have far reaching reputational and compliance consequences. Cyber attacks might be incurred as a result of more strategic business issues (a modern form of boycott or retaliatory measures for perceived business ethic violations) as well as attempts to steal information. Additionally, regulators such as the US Securities and Exchange Commission are formalising their disclosure requirements in relation to cyber security risks and cyber incidents.

The survey results also show that business continuity practitioners are applying BCM to a far wider range of threats than those with which the discipline is traditionally associated. For example, *Business ethics incident*, *new laws and regulations*, the *availability of credit* and *exchange rate volatility* all feature in the planning of BCM practitioners.

This should not be a surprise given that *business resilience* requires a comprehensive approach, one that BCM offers. BCM provides the link between the organization's objective, the risks that it agrees to take, and the measures needed to manage the resulting vulnerabilities.

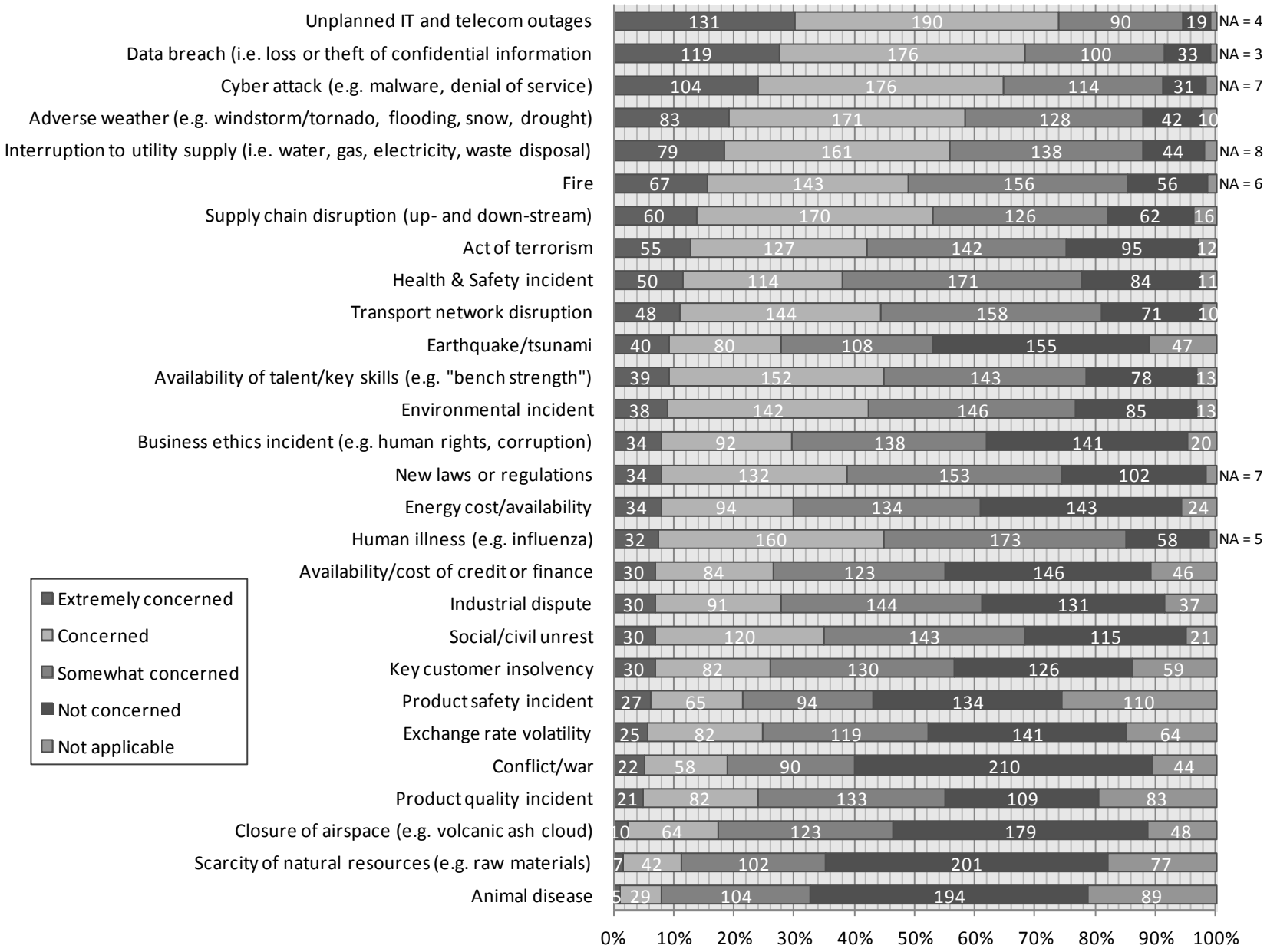
The survey does raise a question as to the extent that individual organisations can deal with these challenges by themselves and the extent to which shifts in public policy are required in order to help businesses. Dealing with the world as it is, BCM can help with exploring alternative strategies in business execution, but governments can do more to mitigate the threat environment through closer international co-operation around critical global infrastructures.

Based on your analysis, how concerned are you about the following threats to your organization in 2012?

The top five threats evaluated through risk assessment, based on those registering *extremely concerned* and *concerned*, are as follows:

- Unplanned IT and telecom outages – 74%
- Data breach (i.e. loss or theft of confidential information) – 68%
- Cyber attack (e.g. malware, denial of service) – 65%
- Adverse weather (e.g. windstorm/ tornado, flooding, snow, drought) – 59%
- Interruption to utility supply (i.e. water, gas, electricity, waste disposal) – 56%

Additional and/more specific risks identified by respondents included: Impact of the 2012 Olympics, raw material prices, social networking (reputational damage), escalation of the euro financial crisis and vandalism/theft.



Base: 458. Multiple responses allowed.

Based on your analysis, how concerned are you about the following threats to your organization in 2012 (Scale 1-4)

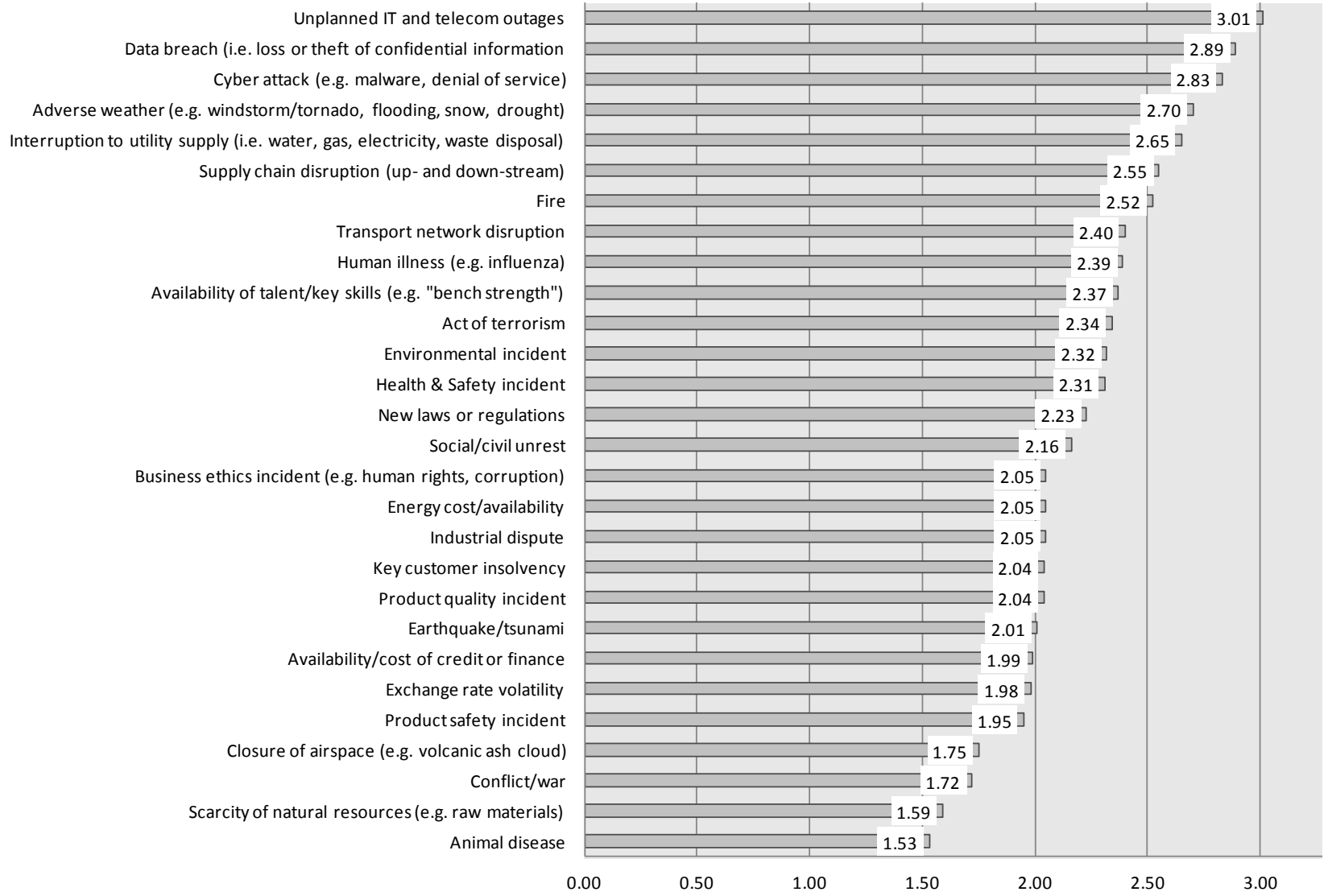
In this chart, each threat is evaluated against scale which translates into a score as follows:

- Extremely Concerned: 4
- Concerned: 3
- Somewhat concerned: 2
- Not concerned: 1

Note: *not applicable* is available as a non-scoring choice.

The highest score would be 4.00 which would equate to 100% of respondents for whom the threat is applicable marking it as *extremely concerned*.

This approach has generated some differences further down the scale where *somewhat concerned* numbers are a significant proportion. For example, *human illness* scores 2.39 or 9th position under this scoring method rather than 17th.



Base: 458. Multiple responses allowed.

Threat evaluation by primary activity of the organization (SIC 2007 sectors)

While there is general consensus around key threats in financial services, information and communications, and professional services, manufacturing places supply chain disruption as their focal point, while *human illness* reaches the top three among public administration sector respondents.

The extent of cross-sector dependencies on underlying IT and Internet infrastructures is otherwise the notable finding from this survey.

Other sectors covered within the overall survey response are *health & social care*, *education*, *retail/ wholesale*, *engineering/ construction*, *entertainment and leisure*, *transport and storage*, *support services*, *mining and quarrying*, and *agriculture, forestry and fishing*.

Sector	Top 3 Threats	"Extremely Concerned" plus "Concerned" (%)	Average score across the full scale (1= not concerned; 4 = extremely concerned)
Financial Services (Base = 124)	• Unplanned IT/telecom outage	80%	3.15
	• Cyber attack	71%	2.99
	• Data breach	68%	2.90
Information & Communications (Base = 77)	• Unplanned IT/telecom outage	81%	3.11
	• Data breach	77%	3.14
	• Cyber attack	75%	3.01
Professional Services (Base = 70)	• Data breach	66%	2.82
	• Unplanned IT/telecom outage	65%	2.87
	• Cyber attack	60%	2.83
Public Administration (Base = 43)	• Adverse weather	74%	2.86
	• Unplanned IT/telecom outage	60%	2.76
	• Human illness	60%	2.64
Manufacturing (Base = 17)	• Supply chain disruption	76%	3.00
	• Unplanned IT/telecom outage	71%	2.82
	• Product safety incident	53%	2.71
Health and Social Care (Base = 17)	• Adverse weather	69%	3.00
	• Data breach	69%	2.94
	• Unplanned IT/telecom outage	63%	3.00
Utilities (Base = 17)	• Cyber attack	82%	3.12
	• Adverse weather	81%	3.13
	• Interruption to utility supply	77%	3.18

Threat evaluation by country of the respondent (top responses)

There is a remarkable consistency across geographical areas in terms of the threats under consideration. However, looking beyond those countries with higher response levels, there are some interesting deviations:

In India, *transport network disruption* was rated at 3.33, followed by *social/civil unrest* at 3.11. Third place belonged to *fire,* which scored 3.00.

In the United Arab Emirates (UAE) *availability of talent /skills* reached third place with a score of 2.88.

Not surprisingly in Japan, consideration of an *earthquake/ tsunami* scored 3.38, in fact every respondent was either *extremely concerned* or *concerned*.

	Top 3 Threats	"Extremely Concerned" plus "Concerned" (%)	Average score across the full scale (1 = not concerned; 4 = extremely concerned)
UK (Base = 167)	• Unplanned IT/telecom outage	71%	2.88
	• Data breach	59%	2.71
	• Adverse weather	58%	2.68
USA (Base = 78)	• Unplanned IT/telecom outage	80%	3.22
	• Data breach	78%	3.11
	• Adverse weather	76%	3.03
Australia (Base = 44)	• Unplanned IT/telecom outage	75%	2.98
	• Adverse weather	68%	2.74
	• Data breach	68%	2.67
Canada (Base = 23)	• Cyber attack	65%	2.68
	• Data breach	57%	2.73
	• Adverse weather	57%	2.64
South Africa (Base =15)	• Unplanned IT/telecom outage	93%	3.43
	• Data breach	87%	3.33
	• Interruption to utility supply	79%	3.07

In 2012, how will investment levels in Business Continuity Management compare to levels in your organization in 2011?

In difficult economic times it is positive to see that BCM investment is holding firm for a majority of respondents and increasing for 25% of them. For 10% it is a different story, facing budget cuts and greater pressures to deliver with fewer resources.

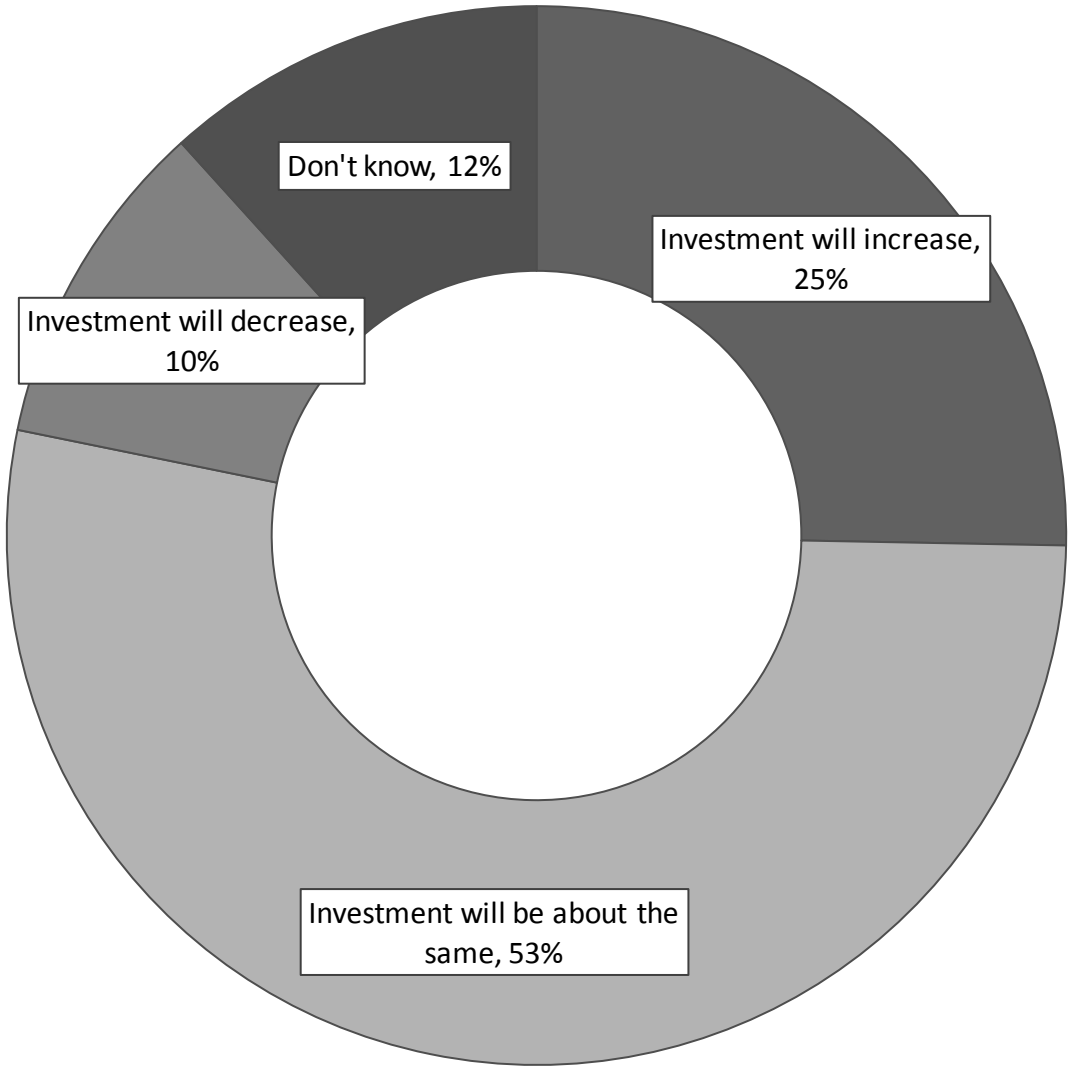
Comments from respondents:

"[I] have to fight for every penny"

"There is a 3% reduction across the board on operational budgets"

"The investment will be higher as a result of the Olympic Games"

"Looking to get more for the same investment"



Base: 454

Business Continuity Institute

About the survey

458 organizations responded to the online survey conducted from 5th to 20th December 2011. The question asked was: "Based on your analysis, how concerned are you about the following threats to your organization in 2012?" Respondents were asked to rate their level of concern against 28 identified threats. Respondents were drawn from 49 countries and 15 industry sectors.

For questions about the survey, contact Lee Glendon CBCI, lee.glendon@thebci.org