BUSINESS CONTINUITY MANAGEMENT

64th RBAP National Convention & General Membership Meeting

29 – 30 May 2017
PRESENTATION OUTLINE

• 2015 Disasters in Numbers
• 2016 & 2017 Top Business Risks
• What is BCM?
• Supervisory Objectives
• BCM Process
• Other Salient Features
• BCM – The Time is Now
2015 Natural Disasters In Numbers

Total of economic damage reported by country (in billion US$)

- United States: 24,88
- China, P Rep: 13,66
- Nepal: 5,17
- United Kingdom: 3,60
- India: 3,30
- Chile: 3,10
- Australia: 2,40
- South Africa: 2,00
- Philippines: 1,90
- France: 1,00

(1): Natural disasters: Epidemic and insect infestations not included
2016 Top Business Risks

Top 10 Global Business Risks for 2016

1. Business interruption (incl. supply chain disruption)
   - 38%

2. Macroeconomic developments (austerity programs, commodity price increase, inflation/deflation)
   - 22%

3. Loss of reputation or brand value

4. Cyber incidents (cyber crime, data breaches, IT failures)
   - 28%

5. Changes in legislation and regulation (economic sanctions, protectionism)
   - 24%

6. Market development (volatility, intensified competition, market stagnation)

7. Market developments (volatility, intensified competition, market stagnation)

8. Changes in legislation and regulation (economic sanctions, protectionism)
   - 11%

9. Theft, fraud and corruption

10. Changes in legislation and regulation (economic sanctions, protectionism)

Executive Summary

The fifth annual Allianz Risk Barometer identifies the top corporate perils for 2016 and beyond, based on the responses of more than 800 risk experts from 40+ countries around the globe.

Business interruption (incl. supply chain disruption), market developments (volatility, intensified competition and market stagnation) and cyber incidents are the top three global business risks. Business interruption (16) is top for the fourth year in succession.

The risk landscape is changing, businesses face a wider range of disruptive forces in 2016 and beyond. The effects of globalization, digitization and technological disruption pose fundamental challenges to many business models.

Businesses and insurers must review their insurance and risk mitigation needs to reflect the new risk management reality. Filling existing, and developing new, risk services will be necessary.

Interconnectedness of risk continues to grow. Many of the top 10 risks such as natural catastrophes, fire, explosion, cyber incidents and political risks can have severe IT implications. Businesses are increasingly concerned about the impact political instability can have on supply chains.

Market developments is the second top risk. Many industrial sectors are facing tougher operating conditions, including intensified competition from new areas.

Businesses are more concerned about cyber incidents, which is the top long-term risk and the peril most likely to increase the threat of M&H. Hardest hit are not the only problem. Operational technology issues also result in major system outages.

Digital and technological innovations and transformations, such as Industry 4.0, bring new risks in addition to benefits. Increasing sophistication of cyber-attacks and the impact of increasing digitalization businesses fear meet. Many companies have insufficient knowledge and budget to mitigate the risk, as the threat continues to evolve.

There are significant differences in the top 10 risks around the world. Macroeconomic developments top the Africa & Middle East rankings. Cyber incidents is the number one risk in the UK.
### Top Business Risks 2017

<table>
<thead>
<tr>
<th>Risk Description</th>
<th>2016 Rank</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business interruption (incl. supply chain disruption and vulnerability)</td>
<td>1</td>
<td>38%</td>
</tr>
<tr>
<td>Market developments (volatility, intensified competition/new entrants, M&amp;A, market stagnation, market fluctuation)</td>
<td>2</td>
<td>34%</td>
</tr>
<tr>
<td>Cyber incidents (cyber crime, IT failure, data breaches, etc.)</td>
<td>3</td>
<td>28%</td>
</tr>
<tr>
<td>Natural catastrophes (e.g. storm, flood, earthquake)</td>
<td>4</td>
<td>24%</td>
</tr>
<tr>
<td>Changes in legislation and regulation (government change, economic sanctions, protectionism, etc.)</td>
<td>5</td>
<td>24%</td>
</tr>
<tr>
<td>Quality deficiencies, vulnerabilities, product recall</td>
<td>8</td>
<td>14%</td>
</tr>
<tr>
<td>Climate change, increasing volatility of weather</td>
<td>6</td>
<td>14%</td>
</tr>
<tr>
<td>Earn damage</td>
<td>8</td>
<td>12%</td>
</tr>
<tr>
<td>Breach, Data security breaches</td>
<td>5</td>
<td>18%</td>
</tr>
<tr>
<td>Environmental risk (e.g. pollution)</td>
<td>5</td>
<td>15%</td>
</tr>
<tr>
<td>Power blackouts</td>
<td>2</td>
<td>17%</td>
</tr>
<tr>
<td>Healthcare (e.g. pandemics)</td>
<td>1</td>
<td>19%</td>
</tr>
<tr>
<td>Machinery breakdown</td>
<td>1</td>
<td>18%</td>
</tr>
</tbody>
</table>
Encompasses policies, standards, facilities, personnel and practices

Covers all sorts of disruptions

Prioritizes critical operations and subsequent efforts to return them to normal

Tailored to the nature, scale, and complexity of a BSFI’s business
SUPERVISORY OBJECTIVES

Ensure Safety and Soundness/Resilience

Sustain Delivery of Financial Services

Preserve Public Trust and Confidence

Mitigate Systemic Risk
BCM - THE TIME IS NOW
IT RISK MANAGEMENT, CYBERSECURITY & CLOUD COMPUTING

64th RBAP National Convention & General Membership Meeting

29 – 30 May 2017
EMERGING THREATS AND RISKS

- Malware
- Ransomware
- Advanced Persistent Threats
- DDoS Attacks
- ATM Malware/ATM Host
- Spoofing
- CNP Fraud
- Phishing
- Spearphishing
IT RISK MANAGEMENT FRAMEWORK

IT RISK MANAGEMENT SYSTEM

IT GOVERNANCE

IT RISK IDENTIFICATION AND ASSESSMENT

IT CONTROLS IMPLEMENTATION

Information Security

Project Management/Development, Acquisition and Change Management

IT Operations

IT Outsourcing/Vendor Management

Electronic Products and Services

IT RISK MEASUREMENT & MONITORING
INFORMATION SECURITY RISK MANAGEMENT

Information Security Governance

Enterprise Risk Management System

People

Technology

Test

Detect

Recover

Respond

Identify

Prevent

Policies and Processes

Cyber Threat Intelligence and Collaboration

Information Security Management
OBJECTIVES OF ISRM

➢ Address technological developments and innovation and dynamic risk profiles
➢ Respond to growing concerns on cyber-attacks and cyber-threats
➢ Introduce a renewed focus on information security both recovery and resumption
➢ Present a holistic framework on ISRM
➢ Heighten expectations of the role of the Board and Senior Management on ISRM
➢ Add provisions on information sharing, collaboration and situational awareness
PROPORTIONATE ADOPTION OF ISRM

- IT Infrastructure and Operations
- Digital/Electronic Financial Products and Services
- IT Projects and Initiatives
- Outsourced Services
- Systemic Importance
- Threats
REQUIREMENTS FOR RURAL BANKS

- IS Governance Including Security Culture
- Security Policies and Procedures
- Identity and Access Management
- Safe Computing Practices
- Hiring Practices
- Security Training and Awareness Programs
- Physical and Environmental Controls
A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Essential Attributes of Cloud Computing

- Resource-Pooling
- Accessible
- On-Demand
- Rapid Elasticity
- Multi-tenancy
- Utilization-tracking
BSP POLICY ACTION ON CLOUD COMPUTING

CORE SERVICES

- Private
- Community
- Hybrid
- Public

NON-CORE SERVICES

- Private
- Community
- Hybrid
- Public
Subsection X162.7 Offshore Outsourcing. Offshore outsourcing exists when the service provider is located outside the country. In addition, offshore outsourcing of bank’s domestic operations is permitted only when the service provider operates in countries which uphold confidentiality.
SUPERVISORY CONCERNS ON CLOUD COMPUTING

- Legal and Regulatory Compliance
- Governance and Risk Management
- Due Diligence/Vendor Management
- Security and Privacy
- Data Ownership and Data Location and Retrieval
- Business Continuity Planning
RATIONALE FOR ALLOWING CLOUD COMPUTING

• Leapfrog financial products & services
• Make innovation more affordable and accessible
• Level playing field
• Focus on core business
• Ensure business continuity and speed-up disaster recovery
When in doubt, Banks should consult BSP before making any significant commitment on cloud computing!
THANK YOU!