Business Continuity Best Practices

Presenters:

Jesse Galindo
Technology Security Consultant
Jesse.Galindo@plantemoran.com
312-602-3537

Cathy Judge
Consultant
Cathy.Judge@plantemoran.com
248-223-3595
Key Learning Concepts:

- Introduction to DRP/BCP
- What’s wrong with current plans?
- Process for Developing an Effective Plan
- Regulatory Authority & Guidance

How long can your organization cope with the loss of its key resources (People, Technology, Facilities, Suppliers & Members)?

What are the critical single points of failure that can impact your institution?

What would be the business impact if critical information was unavailable due to disaster or system failure?

Do you have procedures in place for maintaining your business operations during an unexpected disruption?

To download this presentation, please go to:

http://www.plantemoran.com/Industries/FinancialInstitutions/CreditUnions/
“Disaster Recovery Plan”
- Traditional 1990s terminology
- Included plans for disasters and emergencies
- More event-focused than process-focused
- Often the IT manager or VP Operations’ Responsibility
- Typically testing, was done only at the “EDP Hotsite”

“Business Continuity Plan”
“The business continuity planning process involves the recovery, resumption, and maintenance of the entire business, not just the technology component. While the restoration of IT systems and electronic data is important, recovery of these systems and data will not always be enough to restore business operations.”
- FFIEC Business Continuity Planning Handbook

**FFIEC Definition**
Business continuity planning involves the development of an enterprise-wide BCP and the prioritization of business objectives and critical operations that are essential for recovery. This enterprise-wide framework should consider how every critical process, business unit, department, and system will respond to disruptions and which recovery solutions should be implemented. This framework should include a plan for short-term and long-term recovery operations.
Business continuity planning is required by the regulatory agencies of the FFIEC and guidelines for plan development and maintenance are provided in the FFIEC “Information Technology Examination Handbook, Business Continuity Planning”


Business continuity planning is a sound business practice in any organization – regardless of regulatory requirements.

Events of the past six years have significantly increased the need for concise attention to emergency preparedness:

- Increased dependency on distributed technology, vendors, etc.
- Increased business disasters (power outage, connectivity issues, Internet Banking site down, etc.)
- Increased number of natural disasters (Katrina, tornados, floods, etc.)
- Heightened national alert levels – terrorist threat
Business Continuity Best Practices

What’s wrong with current plans?

- Outdated or gathering dust on the shelves
- Reads like a policy vs. a process to restore
- Recovery team is not aware of plan contents or been trained
- Only addresses restoring IT systems
- Lacks an effective plan to
  - Restore connectivity between locations
  - Manage communications to customers, local media, employees
- Never been tested
- A large single document
- Saved only on the network
- Does not address security incidents
- Too much focus on catastrophic disasters or natural disasters
- Does not address availability of critical vendors
- One plan fits all disruptions
<table>
<thead>
<tr>
<th>Maturity Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FUNDAMENTAL</strong></td>
<td>Responsibilities for continuous service are informal, with limited authority. Management is becoming aware of the risks related to and the need for continuous service. The focus is on the IT function, rather than on the business function. Users are implementing work-arounds. The response to major disruptions is reactive and largely unprepared. Planned outages are scheduled to meet IT needs, rather than to accommodate business requirements.</td>
</tr>
<tr>
<td><strong>TRANSITIONAL</strong></td>
<td>Responsibility for continuous service is assigned. The approaches to continuous service are fragmented. Reporting on system availability is incomplete and does not take business impact into account. There are no documented user or continuity plans, although there is commitment to continuous service availability, and its major principles are known. A reasonably reliable inventory of critical systems and components exists. Standardization of continuous service practices and monitoring of the process is emerging, but success relies on individuals.</td>
</tr>
<tr>
<td><strong>ENHANCED</strong></td>
<td>Accountability is unambiguous and responsibilities for continuous service planning and testing are clearly defined and assigned. Plans are documented and based on system criticality and business impact. There is periodic reporting of continuous service testing. Individuals take the initiative for following standards and receiving training. Management communicates consistently the need for continuous service. High-availability components and system redundancy are being applied piecemeal. An inventory of critical systems and components is rigorously maintained.</td>
</tr>
<tr>
<td><strong>INTEGRATED</strong></td>
<td>Responsibilities and standards for continuous service are enforced. Responsibility for maintaining the continuous service plan is assigned. Maintenance activities take into account the changing business environment, the results of continuous service testing and best internal practices. Structured data about continuous service is being gathered, analyzed, reported and acted upon. Training is provided for continuous service processes. System redundancy practices, including use of high-availability components, are being consistently deployed. Redundancy practices and continuous service planning influence each other. Discontinuity incidents are classified and the increasing escalation path for each is well known to all involved.</td>
</tr>
<tr>
<td><strong>OPTIMIZED</strong></td>
<td>Integrated continuous service processes are proactive, self-adjusting, automated and self-analytical and take into account benchmarking and best external practices. Continuous service plans and business continuity plans are integrated, aligned and routinely maintained. Buy-in for continuous service needs is secured from vendors and major suppliers. Bank-wide testing occurs and test results are fed back as part of the maintenance process. Continuous service cost effectiveness is optimized through innovation and integration. Gathering and analysis of data is used to identify opportunities for improvement. Redundancy practices and continuous service planning are fully aligned. Management does not allow single points of failure and provides support for their remedies. Escalation practices are understood and thoroughly enforced.</td>
</tr>
</tbody>
</table>
Business Continuity Best Practices
The Basics

Critical Business Resources
- People
- Technology
- Facilities
- Suppliers
- Clients

Maximum Allowable Downtime

Availability Solutions
Recoverability Solutions

Current Recovery Capability
- Buy-and-Build
  Identify an alternate site, buy or lease equipment, re-build servers
- Cold Site
  Designate a fully operational data center as alternate site in advance of disaster. Recover similar to Buy-and-Build at designated site
- Warm Site
  Establish alternate site with stand-by hardware and operating systems. Load applications and restore data from tape after disaster
- Hot Site
  Establish alternate site with stand-by hardware and operating system, and applications. Load data on a daily basis from tape
- Hot-Mirrored Site
  Operate two remote data centers both for production processing. Traffic is dynamically routed between sites
# Business Continuity Best Practices

## The Process

<table>
<thead>
<tr>
<th>Phase</th>
<th>Functions</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Foundation</td>
<td>Aligns management and sets expectations, eliminating resistance later in the project.</td>
<td>Purpose, objectives, scope and assumptions</td>
</tr>
<tr>
<td>Business Assessment</td>
<td>Identifies both external and internal threats. Information found in this phase will be the basis for the recovery stages and the BCP Plan</td>
<td>Plan coordinator and development team</td>
</tr>
<tr>
<td>Strategy Selection</td>
<td>Employs recovery procedures to eliminate conditions that would impact operations.</td>
<td>Business impact analysis</td>
</tr>
<tr>
<td>Plan Development</td>
<td>Puts together a choreographed sequence of actions to mitigate the identified threats and risks and ensures recoverability of key services.</td>
<td>Strategy identification and strategy selection</td>
</tr>
<tr>
<td>Implement, Test, Assess, Maintain</td>
<td>Implements the BCP, ensures that the BCP works, assess the BCP against published standards and keeps it current.</td>
<td>Document business continuity plan</td>
</tr>
</tbody>
</table>

8

---

**plante moran**
Business Continuity Best Practices
1. Mission, Objectives, Scope & Assumptions

- **Mission & Objective** - Examples
  - The most important objective of business continuity planning is to protect the “Bank” if all or parts of its operations or computer services are disrupted by a disaster. The planning process should reduce to a minimum, the disruption of operations and ensure some level of organizational stability during an orderly recovery after a disaster.
  - Other possible objectives are: Manage successfully through a disaster, meet regulatory and contractual requirements, ensure continuation of branch operations.

- **Assumptions** - Examples
  - The plan is designed to recover from the "worst case" destruction of the “Bank” operating environment. The worst case includes any non-data processing function that may be in close proximity to the data center or workstations.
  - This plan is not designed for the “worst case” destruction, but focuses on the loss of recovery of key components such as local application, network, etc.
  - Fiserv is responsible for the availability of core applications (such as ITI) and thus not addressed in this plan.
  - The plan is based upon a sufficient number of staff not being incapacitated to implement and affect recovery. Therefore, the level of detail of the plan is written to a staff experienced in the “Bank’s” computer services.
  - Development, testing and implementation of new technologies and applications are suspended so that all resources are available to recover existing critical production processing.
  - An alternate site (backup computer facility) in which to establish recovery of computer processing may be necessary. Time frame requirements to recover computer processing are significantly less than estimated times to repair/reconstruct a data center on an emergency basis.
  - The computer facilities of the alternative site is not within the scope of this plan and is assumed not to be impacted by any disaster which may interrupt computer operations at “Bank” offices.
Characteristics of BCP Coordinator:
- Should have authority
- Should have available time / resources
- Should be able to communicate with technical staff and non-technical staff
- Should be organized, detail-oriented and a competent writer
- Fluent in project management principles and techniques
- Will need highly developed qualities of patience, perseverance and diplomacy
- Coordinators need to cultivate enthusiasm and constantly reinforce the buy-in of plan participants

The makeup of your team will vary depending on the size of your IT organization, business unit and the number of departments involved

Determine active team members and advisory team members - from functional areas such as:
- Security (data & physical)  Senior Management  Branch Operations
- Customer Service  Human Resources  Risk Management
- IT  Lending  Trust
- Facilities  Executive area  Compliance
Business Continuity Best Practices

3. Project Plan

- **Formal project plan to develop your BCP plan**
  - Treat it like you would any other project with formal plan, team, responsibilities, timelines, budget, etc.
  - Don't let it be a passive project
  - Assign a strong project manager
  - Develop key timelines and milestones
  - Involve a team that represents your organization
  - Sponsorship at the executive level is critical
  - Allocate appropriate resources
  - Don't let software drive the project

- **Hire outside help (project managers, consultants, etc.)**
  - Facilitate the process & not write the plan for you
  - Strong tools & methodologies
  - Experience with financial institutions
  - Be wary of consultants that push towards a product or recovery site (do what's right for you)
  - Bring strong project management skills (will keep the project on course)
Prior to developing Plan

- Review existing DRP plan
- Review internal plans and policies:
  - Evacuation plans
  - Security procedures
  - Fire protection plan
  - Insurance program
  - Safety & health program
  - Risk management plans
- Meet with outside groups – Ask about potential emergencies and available resources for responding to them. For example, one facility discovered that a dam 50 miles away posed a threat. Familiarize the local emergency agencies with your facility and any specific needs:
  - Local emergency management office
  - Police department
  - Utility companies – communication lines, water, electric, etc.
  - Other local organizations that could present potential threats to Bank
- Identify your internal resources & capabilities:
  - Personnel – facilities manager, electrician, network administrator, etc.
  - Equipment – fire protection, communications, emergency power, etc.
  - Facilities – emergency operating center, etc.
  - Back-up processes – arrangements with other facilities or organizations to provide for critical operations such as payroll, communications, etc.
- Review insurance policy for adequate coverage for infrastructure and recovery costs
- Conduct data-center / facility assessment
Business Continuity Best Practices
4. Threat Assessment

- Risk evaluation involves determining the events that can adversely affect the Bank’s operations, the damage such events can cause and the measures needed to prevent or minimize the effects of potential loss.

- Risk evaluation would include:
  - Threat identification
  - Determine probability / occurrence
  - Determine severity / impact
  - Identify preventive measures in place
  - Identify preventive measures improvement opportunities

<table>
<thead>
<tr>
<th>Common Natural Disasters</th>
<th>Common Business Disasters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Earthquakes</td>
<td>Communications/Network Failure</td>
</tr>
<tr>
<td>Hurricanes</td>
<td>Hardware Failure</td>
</tr>
<tr>
<td>Floods / Mud Slides</td>
<td>Power Failure</td>
</tr>
<tr>
<td>Tornados</td>
<td>Software Failure or Corruption</td>
</tr>
<tr>
<td>Lightning</td>
<td>Flood</td>
</tr>
<tr>
<td>Extreme Weather</td>
<td>Fire</td>
</tr>
<tr>
<td></td>
<td>Human Errors</td>
</tr>
</tbody>
</table>
The following chart presents the types of events which have forced companies to declare a disaster:

<table>
<thead>
<tr>
<th>Event</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power failure</td>
<td>42%</td>
</tr>
<tr>
<td>IT hardware failure</td>
<td>31%</td>
</tr>
<tr>
<td>Network failure</td>
<td>21%</td>
</tr>
<tr>
<td>IT software failure</td>
<td>16%</td>
</tr>
<tr>
<td>Human error</td>
<td>16%</td>
</tr>
<tr>
<td>Flood</td>
<td>12%</td>
</tr>
<tr>
<td>Hurricane</td>
<td>10%</td>
</tr>
<tr>
<td>Fire</td>
<td>7%</td>
</tr>
<tr>
<td>Winter storm</td>
<td>6%</td>
</tr>
<tr>
<td>Terrorism</td>
<td>4%</td>
</tr>
<tr>
<td>Earthquake</td>
<td>3%</td>
</tr>
<tr>
<td>Tornado</td>
<td>2%</td>
</tr>
<tr>
<td>Chemical spill</td>
<td>1%</td>
</tr>
<tr>
<td>Other</td>
<td>12%</td>
</tr>
<tr>
<td>Don't know</td>
<td>4%</td>
</tr>
<tr>
<td>Never declared a disaster</td>
<td>24%</td>
</tr>
</tbody>
</table>

Base: 250 disaster recovery decision-makers and influencers at businesses worldwide (multiple responses accepted)

Source: Forrester Research, Inc.
Recovery procedures are staged around the most critical resource (with the shortest MAD) to the application with the longest MAD.

<table>
<thead>
<tr>
<th>Application Name</th>
<th># of users</th>
<th>Usability</th>
<th>Essential</th>
<th>Delayed</th>
<th>Suspended</th>
<th>Recovery Strategy (Essential, Delayed, Suspended)</th>
<th>Maximum Allowable Downtime</th>
<th>What would you do if the system was not available?</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChexSystems</td>
<td>~900 Daily</td>
<td>MD MD MD MD MD MD MD CT</td>
<td>Suspended 60 days</td>
<td>pull credit report or alter process for validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deluxe Checks</td>
<td>~900 Daily</td>
<td>MN MN MN MN MN MN MN MN</td>
<td>Suspended n/a</td>
<td>mail check orders</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Insight</td>
<td>~3500 Daily</td>
<td>MN MN MN MN MN MN MN MN</td>
<td>Essential 48hrs</td>
<td>Use phone banking or come to branch</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bill Payment</td>
<td>3,000 Daily</td>
<td>MN MN MN MN MN MN MN MN MN</td>
<td>Suspended N/A</td>
<td>use other report writers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Core Banking System</td>
<td>~200 Daily</td>
<td>MD CT</td>
<td>Delayed 4 days</td>
<td>customers can pay their bills other ways</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust Metavante</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Watchdog OFAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WirePro</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### CURRENT STRATEGY

<table>
<thead>
<tr>
<th>Recovery Strategy</th>
<th>Buy-and-Build</th>
<th>Cold Site</th>
<th>Warm Site</th>
<th>Hot Site</th>
<th>Hot-Mirrored Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify an alternate site, buy or lease equipment, re-build servers</td>
<td>Designate a fully operational data center as alternate site in advance of disaster. Recovery similar to Buy-and-Build at designated site</td>
<td>Establish alternate site with stand-by hardware and operating systems. Load applications and restore data from tape after a disaster</td>
<td>Establish alternate site with stand-by hardware, operating system, and applications. Load data on a daily basis from tape</td>
<td>Operate two remote data centers both for production centers. Traffic is dynamically routed between sites</td>
<td></td>
</tr>
<tr>
<td>Recovery Time</td>
<td>5 days or more</td>
<td>More than two days, exact time depends upon hardware availability</td>
<td>24 to 36 hours</td>
<td>3 to 12 hours</td>
<td>Instantaneous</td>
</tr>
<tr>
<td>Technical Architecture</td>
<td>None</td>
<td>Data center with environmental controls and telecommunications</td>
<td>Load applications and restore data from tape during a disaster</td>
<td>Restore data from tape on a daily basis before a disaster</td>
<td>Mirroring Load Balancing</td>
</tr>
<tr>
<td>Key Benefits</td>
<td>Inexpensive</td>
<td>Accommodates web-based systems Inexpensive</td>
<td>Can use as alternate site for development and lab Good compromise between recovery time and cost</td>
<td>Reliable recovery method Rapid recovery of critical applications</td>
<td>Instantaneous recovery Risk of data loss limited to last few uncommitted transactions Operational efficiencies</td>
</tr>
<tr>
<td>Key Weaknesses</td>
<td>Potentially unreliable Can not accommodate web-based systems May take up to a week to recover</td>
<td>Potentially unreliable May take up to a week to recover Loss of data since most recent back-up</td>
<td>If servers are used for development recovery may be hindered by configuration changes Loss of data since most recent back-up</td>
<td>Can't use alternate site for test or lab purposes Expense Loss of data since most recent back-up</td>
<td>Expensive Potentially complex to operate</td>
</tr>
</tbody>
</table>

### Business Continuity Best Practices

#### 6. Strategy Analysis

- **Buy-and-Build**
  - Identify an alternate site, buy or lease equipment, re-build servers
  - Designate a fully operational data center as alternate site in advance of disaster. Recovery similar to Buy-and-Build at designated site
  - Recovery Time: 5 days or more
  - Technical Architecture: None
  - Key Benefits: Inexpensive
  - Key Weaknesses: Potentially unreliable Can not accommodate web-based systems May take up to a week to recover

- **Cold Site**
  - Establish alternate site with stand-by hardware and operating systems. Load applications and restore data from tape after a disaster

- **Warm Site**
  - Load applications and restore data from tape during a disaster

- **Hot Site**
  - Restore data from tape on a daily basis before a disaster

- **Hot-Mirrored Site**
  - Operate two remote data centers both for production centers. Traffic is dynamically routed between sites
  - Mirroring Load Balancing
  - Reliable recovery method
  - Instantaneous recovery
  - Risk of data loss limited to last few uncommitted transactions
  - Operational efficiencies
Selecting your off-site vendor:

- **Reputation** – How long has the facility been in existence? Have you checked their financial statements?
- **Site Security** – Security at storage facility should be no less stringent than your own facility. Some questions to consider:
  - What are the access controls in the facility?
  - Is visitor access restricted?
  - Are client names concealed, even from one another?
  - Security measures during transportation of media? (unmarked cars, security in vehicles, employee monitoring, etc.)
  - How are employees screened?
  - Are cameras or other devices used to monitor facility traffic?
  - How are emergency calls handled?

- **Media Management** – A very important factor, how the facility manages client records, may present the following questions:
  - How is media of several clients segregated?
  - Is media transported in plastic containers or cardboard boxes?
  - What kind of inventory management system is used?
  - Are employees trained in proper media handling?
  - What controls exist to monitor flow of media in and out of the facility?

- **Environmental Factors** – detection, prevention and suppression controls for smoke, fire, water, humidity, etc.
  - What capabilities are installed to detect smoke, heat, flame, water, and intrusion?
  - What suppression systems exist?
  - Is the alarm system tied directly to fire, police, and security services?
  - How are temperature, heat, humidity and contamination controlled?
  - How often are environmental controls tested?

- **Transportation** – Tapes and records are at higher risk of loss or damage while riding in the back of a van
  - Is media transported by vendor employees or independent contractors?
  - Is media subjected to ambient climate conditions?
  - Are vehicles equipped with antitheft devices?
Finally time to document plan:

- It is imperative to commit the Business Continuity Plan to writing, otherwise:
  - Planning will be forgotten when an incident occurs
  - There will be no consistency to actions and responses taken
  - There will not be a baseline to update and improve over time and as changes occur
  - Many sites are dependent upon other sites for production and network function – there needs to be a common understanding of what will be done at the various Bank sites to preserve Business Continuity
  - Regulatory compliance

- Plan Structure
  - Logically segregated sections
    - Administrative sections: Team, roster, responsibilities, when to declare a disaster, incident response policy, etc.
    - Policies: Incident response policy, plan maintenance policy, plan testing policy, etc.
    - Asset Inventory: Application listing, vendor information, network diagrams, etc.
    - Analysis: Threat Assessment, Business Impact Analysis, etc.
    - Recovery Steps: Systems recovery/restoration, etc.
    - Continuity of Operations: Branch operations, lending, etc.
    - Attachments: Damage assessment, sample press release, phone redirect, phone greeting, etc.

- Plans can be segregated by:
  - Duration of disruption: 24hrs, 72hrs, 5 days
  - Type of disruption: Systems, neighborhood, branch-level, etc.
  - Type of disaster: Fire, communication break, etc.
8. Implementation / Maintenance

- **Security** - Because of the sensitive nature of the information your plan will contain, it’s suggested that only recovery team members should be given copies of your plan.

- **Plan storage**
  - Single document vs. fragmented
  - Physical copy vs. electronic copy
  - On CDs vs. Internet

- **Copies of the plan should be easily accessible**
  - Several copies of the plan should be stored off-site in a secure location
  - If plan is distributed online, make sure that hosting is separate from the production environment
  - Key employees may need access to the plan during non-working hours
  - Each plan should be kept current, dated and version controlled
  - If software program has been used to assist with plan development, copies of the planning disks and program should be stored off-site

- **Maintaining the plan is as important as writing the plan itself**
  - Most recovery plans are not maintained. Within a year or less, the plan becomes outdated, as staff have changed, the infrastructure has changed, the vendors have changed, etc.
  - Present parts of the plan to those who assisted in creating the plan initially for updates
  - Institute a maintenance plan that includes automatic reminders where each section is designated with the frequency (quarterly, annually, etc.)

- **The board is required to review and approve the plan annually**
9. Testing the Plan

- **Checklist testing (also known as walk-thru)**
  - Determines whether the plan is adequate, i.e., the recovery team reviews the plan and identifies key elements that should be up-to-date and available, the telephone number listings are current, copies of plan are stored at all the right locations, the inventory of systems is accurate, the risk assessment is current, etc.
  - Advantages: It is cheap, involves minimal interruption to business, can usually be arranged with short notice, it is a gentle way to explore and test the plan
  - Disadvantage: It has limited training value, the test lacks realism

- **Non-business interruption test (also known as role-play)**
  - A disaster is simulated so that normal operations are not interrupted. The following areas are adequately tested: hardware, software, telecommunications, supplies, etc.
  - Advantages: Good training value, challenges the participants and plan
  - Disadvantages: The role-play can move towards extreme

- **Parallel Testing**
  - Under this scenario the systems (with preceding day’s backup data) are restored at alternate site and current days transactions processed
  - All reports normally produced at the alternate location for the current day should agree with those reports at your normal business location
  - Advantages: excellent training value, tests the recovery of key systems
  - Disadvantages: It will be costly

- **Business Interruption Testing (pull the plug)**
  - This tests the total business continuity plan
  - This test is costly and could disrupt your normal business operations, so proceed with caution
  - Adequate time must be allocated for this test
  - You may want to test only certain portions of the plan initially to identify the workability of each part prior to attempting the full test
Business Continuity Best Practices
Regulatory Authority & Guidance

- FFIEC Business Continuity Planning (BCP) Booklet (March 2008)

- Disaster Preparedness & Response Examination Procedures
  NCUA Letter to Credit Unions (08-CU-12)

- NCUA Risk Alert
  Disaster Planning and Response (06-RISK-01)
  www.ncua.gov/RiskAlert/2006/06-Risk-01.doc

- Guidance on Pandemic Planning
  NCUA Letter to Credit Unions (08-CU-01)
  www.ncua.gov/letters/2008/CU/08-CU-01Encl.doc

- Influenza Pandemic Preparedness
  NCUA Letter to Credit Unions (06-CU-06)
  www.ncua.gov/letters/2006/CU/06-CU-06.pdf
GLBA 501(b)

- **Security Guidelines**
  “As stated in section 501, these safeguards are to:
  (1) Insure the security and confidentiality of customer records and information;
  (2) Protect against any anticipated threats or hazards to the security or integrity of such records; and
  (3) Protect against unauthorized access to, or use of, such records or information that would result in substantial harm or inconvenience to any customer”

- “These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information”

- **Therefore:** Security Standards do not specifically state that the Bank’s Information Security Program need address threats to information availability

- **However,** management’s Risk Assessment(s) should consider threats to Security, Integrity and Availability
Be Informed

Some of the things you can do to prepare for the unexpected, such as making an emergency supply kit and developing a family communications plan, are the same for both a natural or man-made emergency.

However, there are important differences among potential emergencies that will impact the decisions you make and the actions you take. Learn more about the potential emergencies that could happen where you live and the appropriate way to respond to them.

In addition, learn about the emergency plans that have been established in your area by your state and local government.

Emergency preparedness is no longer the sole concern of earthquake prone California and those who live in the part of the country known as "Tornado Alley." For Americans, preparedness must now account for man-made disasters as well as natural ones, knowing what to do during an emergency is an important part of being prepared and may make all the difference when seconds count.
Hazards Assessment is intended to provide emergency managers, planners, forecasters and the public advance notice of potential hazards related to climate, weather and hydrological events. It integrates existing National Weather Service official medium (3-5 day), extended (6-10 day) and long-range (monthly and seasonal) forecasts and outlooks, and hydrological analyses and forecasts, which use state-of-the-art science and technology in their formulation.
Thank You

To download this presentation, please go to:
http://www.plantemoran.com/Industries/FinancialInstitutions/CreditUnions/

Presenters:
Plante & Moran PLLC

Jesse Galindo
Technology Security Consultant
Jesse.Galindo@plantemoran.com
312.602.3537

Cathy Judge
Consultant
Cathy.Judge@plantemoran.com
248-223-3595

www.plantemoran.com