

## Business Continuity & Disaster Recovery:

### Preparing Your Business for the Unexpected

December 9, 2011

## A Corporate-Bank Partnership

Daniel J. McCarty  
Senior Vice President  
PNC Bank

# Ideas To Be Addressed

---

**Disruptive Events: Some Examples**

**Corporate Risk Factors to be Considered**

**Business Resiliency: A Bank's Approach**

**Focus for Financial Contingency Planning:  
Corporate-Bank Interactions**

**Recommendations**

**Final Comments**

# Disruptive Events...

## ...Some Examples

# Disruptive Events... Some Examples

---

## September 11<sup>th</sup>: Too Many to Mention

- Cantor Fitzgerald
- Check 21 and the Fed
  - Wire Systems
  - Check Clearing
  - Funding

## Key Executives

- Amazon.com
- Tesla Motors
- Another Banking Situation

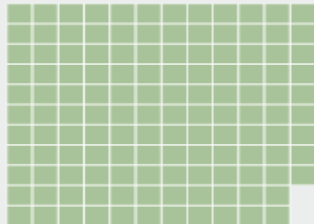
## Key Processes and Operating Systems

- Katrina and Hibernia Bank
- Power Outage: August 14, 2003 at 4:10pm ET
- Data Breaches: TJX, Heartland, Sony, Card Systems...

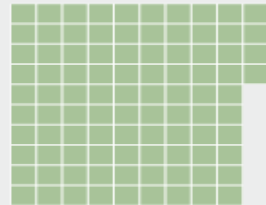
# Disruptive Events... Data Breaches

■ = 1 million records lost, colored by breach type (hack, stolen, lost, or fraud)

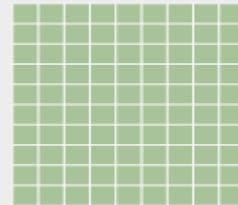
Heartland Payment Systems  
**130m records lost** – Hacked  
 January 20, 2009



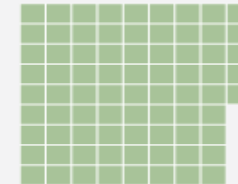
TJX Companies, Inc.  
**94m** – Hacked  
 January 17, 2007



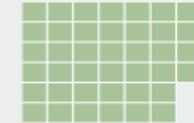
TRW  
**90m** – Hacked  
 June 1, 1984



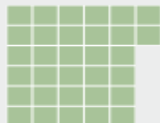
Sony Corporation  
**77m** – Hacked  
 April 26, 2011



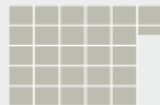
CardSystems  
**40m** – Hacked  
 June 19, 2005



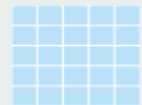
RockYou, Inc.  
**32m** – Hacked  
 Dec. 14, 2009



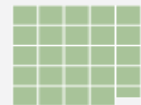
US Dept. of Veterans Affairs  
**26m** – Stolen  
 May 22, 2006



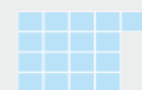
HM Revenue and Customs  
**25m** – Lost  
 Nov. 20, 2007



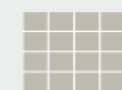
Sony Corporation  
**25m** – Hacked  
 May 2, 2011



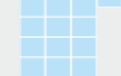
T-Mobile  
**17m** – Lost  
 Oct. 6, 2008



Canada Revenue Agency  
**16m** – Stolen  
 Nov. 1, 1986



Bank of New York  
**12m** – Lost  
 Sept. 6, 2008



GS Caltex  
**11m** – Lost  
 Sept. 6, 2008



Dai Nippon Printing Company  
**9m** – Fraud  
 March 12, 2007



Fidelity National Info. Services  
**8m** – Fraud  
 July 3, 2007



TD Ameritrade  
**6m** – Hacked  
 Sept. 14, 2007



Chilean Ministry of Education  
**6m** – Hacked  
 May 11, 2008



Data Processors International  
**5m** – Hacked  
 Dec. 8, 2008



According to DataLossDB

# Corporate Risk Factors

# Corporate Risk Factors: What are They?

---

- Credit
- Operational
- Market
- Reputational
- Regulatory
- Environmental
- Priorities.... You need them!

# Business Resiliency

## A Bank Approach

# Business Resiliency: A Bank Process

---

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

# Business Resiliency: A Bank Process

---

## Program Components

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

# Business Resiliency: A Bank 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 Resiliency: A Bank 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 Resiliency: A Bank 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

# Focus for Financial Contingency Planning

Corporate-Bank Interactions

# Focus for Financial Contingency Planning

## 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?

# Focus for Financial Contingency Planning

## Disbursements

- Demand Accounts (Checking):
  - Authorized signers/resolutions: Limits, number of signers, physical location: Do you have paper and electronic copies?
  - Check stock: Accessable?
  - 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

# Focus for Financial Contingency Planning

## 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

# Recommendations

# Recommendations

## 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

# Recommendations

## 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!!!!**

Thank You!