Industry Cluster Briefings Series

FINANCIAL SERVICES CLUSTER

INSIDE

Overview

Within the Financial Services Industry Cluster, Hurricane Sandy added an unwelcome addition to the many headaches that have been crimping financial industry profits. Many banks were still in the midst of working out mortgages that went sour during and after the financial crisis. On top of that there were lost revenues from fees banks waived after the storm, such as late penalties and ATM surcharges. Also banks lost real estate closings and refinancing transactions that were cancelled because of the storm.[1] The insurance industry had also been facing record low interest rate returns on premium investments prior to the substantial claims due to damage caused by Sandy. The Financial Services Industry Cluster falls under three main categories due to the nature of their transactions[2]:

Business Continuity Overview for the Financial Services Industry Cluster

Business Continuity is the creation of a plan to resume critical business processes after a disruption. Having a plan in place before a disruption, and practicing the plan, will enable a business to resume critical processes much more swiftly, efficiently and cost-effectively than an improvised response. According to FEMA, 75 percent of businesses that do not have BCPs fail within three years of a natural disaster.[1]

Regulatory compliance is a significant factor influencing the development of this industry's business continuity strategies. Moreover, while business continuity or disaster recovery regulations may not apply in every business situation, a general understanding of legislation governing data integrity, availability and compliance is helpful for any organization developing a Business Continuity strategy. *(cont. page 2)*

[1] http://www.nj.com/business/index.ssf/2013/01/new_jerseys_banks_bracing_for.html
[2] http://www.usfa.fema.gov/pdf/efop/efo47103.pdf

(cont. from page 1)

There are two types of regulations[3]:

1. Standards and requirements that must be met in order to provide competitive pricing and a high level of service to customers. An example may be complying with ISO 9000 standards.
2. Government regulations imposed on specific industries that must be adhered to in order to do business. These regulations are created to protect the security of institutions and create national standards of uniformity. The Financial Services Industry is particularly sensitive to a government-imposed regulatory environment, and firms in the industry must consider regulations about security of information and safety of government-insured funds, along with compliance with government regulatory bodies, when developing Business Continuity Plans.

The following are the Primary Government regulations which pertain to the Financial Service industry cluster that must be considered when developing a Business Continuity Plan:

Regulation	Impact on Business Continuity	Notes
Sarbanes-Oxley Act[4]	Corporate officers are liable for business continuity	Relevant for publicly held companies in the U.S.
IRS Procedure 86-19[5]	Requires off-site protection and documentation of computer records of tax information	Records must be available in the event that the primary facility is subjected to unplanned outage
Consumer Credit Protection Act (CCPA) Section 2001 Title 1X[6]	Due diligence for availability of data in Electronic Funds Transfers including Point of Sale	Redundant data storage and processing capability is critical
Foreign Corrupt Practices Act 1977[7]	Publicly held corporations must provide "reasonable protection" for IT systems	Holds management accountable to have IT continuity systems in place

[3] www.geminare.com/pdf/U.S._Regulatory_Compliance_Overview.pdf
[4] http://www.soxlaw.com/
[5] www.irs.gov/pub/irs-drop/rp-09-19.pdf
[6] http://www.fdic.gov/regulations/laws/rules/2000-50.html
[7] www.justice.gov/criminal/fraud/fcpa/docs/fcpa-english.pdf

Business Continuity Planning continued

A financial institution's business continuity planning process should reflect the following objectives[8]:

- The business continuity planning process should include the recovery, resumption, and maintenance of all aspects of the financial institution, not just recovery of the technology components.
- Business continuity planning involves the development of an enterprise-wide Business Continuity Plan (BCP) and the prioritization of business objectives and critical operations that are essential for recovery
- Business continuity planning includes the integration of the institution's role in financial markets before, during, and after a disaster
- Business continuity planning should include regular updates to the BCP based on changes in business processes, audit recommendations, and lessons learned from testing
- Business continuity planning represents a cyclical, process-oriented approach that includes a business impact analysis, a risk assessment, risk management, and risk monitoring and testing.

Common risks and potential actions to reduce those risks for Financial Services companies are identified below[9]:

Risk	Potential Protective action
Lack of telecommunications, transportation, electricity, etc.	• Multiple redundant services and proximity of vendors and service providers to the disaster area
Denial of access to facilities	• Integrate remote access into operations. Ability to work from home for employees could decrease staffing problems during a disaster.
Lack of internet/telephone lines in disaster site	• Utilize several disparate locations for database backup and services; utilize cloud technology
Power outage	• Invest in and regularly test emergency generators at institutions and alternative work locations
Telecommunications provider outage	• Consider using more than one provider, again in separate locations

(continued on page 4)

[8] http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

[9] http://www.sec.gov/about/offices/ocie/jointobservations-bcps08072013.pdf

Risk	Potential Protective action
Loss of communication with clients and staff	• Take measures to ensure website is updated with status of operations. • Introducing firms should consider publishing contact information for clearing firms on their websites to enable customers to execute liquidating orders or wire transfers through their clearing firms should the firm be inoperable. • Firms should consider implementing a communication plan that allows firms to better communicate and coordinate with regulators, exchanges, emergency officials and other firms
Vendor Relationship	• Consider examining whether vendors that provide critical services such as clearance and settlement, banking and finance, trading support, fuel, telecommunications, electricity and other utilities also have adequate BCPs. • Consider categorizing vendors (low-risk, high-risk, etc.) and evaluate the risk in BCP plans. Firms should contemplate having pre-arranged contracts in place with multiple suppliers and schedule deliveries in advance of an event.
Regulatory Considerations	• Firms should consider time-sensitive regulatory requirements, since a crisis event can occur at any time. For example, some firms put a lower prioritization on month-end financial processes, which increased challenges due to the storm's proximity to month end, and caused delays in firms' production of certain month end data for regulatory computations and financial reporting[10].
Vandalism and/or theft	• Develop plans with local law enforcement and emergency management to maintain security during a prolonged absence. • Invest in remotely accessed security and surveillance equipment.
Physical damage	• Develop contact lists of construction contractors, roofers, plumbers, landlords, building management etc. who can reliably respond to physical damage.
Loss of customer confidence	• Keep status of business updated on social media and the business' website; inform local media that your business survived the event. Reach out to current customers via email blasts and courtesy calls (if possible). If the location is no longer accessible, search for a temporary location nearby and publicize that address.

[10]http://www.federalreserve.gov/newsevents/press/bcreg/20121030a.htm

More information on business continuity can be found at these sources:

- FEMA Preparedness for Businesses
- SBA Disaster Planning
- FEMA: Ready.gov
- Red Cross Ready Rating
- Institute for Business and Home Safety

Many financial services businesses will likely need a more complex BCP; examples of such BCPs can be found in the following links:

- IBHS Decision Track
- IBHS Advanced Tack Resources
- IBHS Supply Chain
- IBHS Logistics
- IBHS Incident Management and Crisis Communication
- IBHS Vulnerability Assessment
- IBHS Financial Controls and Resiliency
- IBHS Employee Awareness, Training, and Exercises

A reliable Business Continuity Plan (BCP) should be developed using a systematic, orderly approach. The questions below include processes any BCP should address.

Key Questions	How to proceed
What are our most critical processes?	Think of processes that are customer-facing, employee-facing or facilitate cash-flow.
Who performs these processes?	Create an employee call tree or employee accountability and notification system.
What do they need to perform these processes?	Create a list of critical tools, supplies, data sources, etc.
Where can the people who perform our critical processes work if our business-as-usual facility is unavailable?	If possible enable employees to work from home, put in place an agreement with similar businesses to reciprocally provide emergency workspace, create a list of local realtors who have appropriate space to lease.
How well do you and your employees know your plan?	Have all involved walk through the steps of the plan in a tabletop exercise. Identify gaps in the plan and fix them. Document fixes. Do this annually and this basic plan will be kept up-to-date and will improve over time.

Hazard Mitigation for the Financial Services Industry Cluster

Hazard Mitigation is the assessment of the hazards that are most likely to strike a particular business type or location, and the creation of a plan to lessen the effect of those hazards before they strike[2]. The most common example of hazard mitigation is a fire alarm: the vast majority of all construction is vulnerable to fire, and advance warning of a fire hugely diminishes the risk of loss of life or property.

Each business should plan for the hazards they are most likely to face for example, a business in the Midwest is not likely to experience storm surge from a hurricane, so hurricane mitigation should be a lesser priority. Hazard mitigation is distinct from business continuity planning; hazard mitigation activities are undertaken before a disruption to physically reduce the effect or damage on the business. Hazard mitigation tools and resources are available from the following link to FEMA.

Examples of Potential Hazards	Examples of Mitigation Actions
Flooding	• Build with flood damage resistant materials: http://www.fema.gov/media-library-data/20130726-1503-20490-6330/fema15.pdf • Raise electrical system components: http://www.ready.gov/floods • Anchor fuel tanks • Install sewer backflow valves • Elevate buildings in low lying areas • Consider utilizing the National Flood Insurance Program (NFIP): http://www.fema.gov/national-flood-insurance-program
Loss of Power	• Invest in and regularly test an emergency generator: http://www.emd.wa.gov/preparedness/GeneratorSafety.shtml • Have battery-operated light sources on hand, keep stock of batteries: http://www.ready.gov/blackouts • Invest in an Uninterruptible Power Supply (UPS): http://www.energystar.gov/index.cfm?c=new_specs.uninterruptible_power_supplies, http://en.wikipedia.org/wiki/Uninterruptible_power_supply • Plug computer and electronic equipment into surge protectors: http://www.disastersafety.org/blog/surge-protector-and-power-strip-know-the-important-difference/ • Unplug any sensitive electronic equipment in advance of severe storms

[2]http://www.fema.gov/what-mitigation/federal-insurance-mitigation-administration

Hazard Mitigation continued:

Examples of Potential Hazards	Examples of Mitigation Actions
Strong Winds	• Utilize Exterior Insulation and Finish System (EIFS): http://www.fema.gov/media-library-data/20130726-1627-20490-4852/how2027_eifs_walls_4_11.pdf • Elevate items in house/business that could flood; bring in items from outdoors that could become projectiles: http://www.ready.gov/severe-weather • Protect windows and doors with covers: http://www.ohsep.louisiana.gov/factsheets/avoidingwinddamage.pdf • Reinforce or replace garage/loading doors • Secure metal siding and metal roofs • Secure built-up and single-ply roofs • Secure composition shingle roofs • Brace gable end roof framing
Fire	• Eliminate electrical outlet overloads: http://www.usfa.fema.gov/citizens/home_fire_prev/ • Test smoke detectors regularly: http://www.ready.gov/fires • Replace long-term use of extension cords with permanent wiring • Replace broken or frayed electrical cords • All employees now how and where to shut off electrical power • Separate incompatible materials (flammables and corrosives): http://www.lbl.gov/ehs/chsp/html/storage.shtml • Keep flammables in approved safety containers: https://www.osha.gov/dte/library/flammable_liquids/flammable_liquids.html • Use flammable liquids only in well-ventilated areas

Insurance Considerations Specific to the Financial Services Industry Cluster

Insurance is an important component of the business continuity planning process. It can allow management to recover losses that cannot be completely prevented and expenses related to recovering from a disruption. Generally, insurance coverage is obtained for risks that cannot be entirely controlled, yet represent a potential for financial loss or other disastrous consequences. Available insurance options should be reviewed to ensure that appropriate insurance coverage is provided given the risk profile of the institution. Institutions should perform an annual insurance review to ensure that the level and types of coverage are commercially reasonable and consistent with any legal, management, and board requirements. Insurance can reimburse an institution for some or all of the financial losses incurred as the result of a disaster or other significant event. To facilitate the claims process, institutions should create and retain a comprehensive hardware and software inventory list in a secure off-site location and detailed expenses should be documented to support insurance claims. Additional considerations include:

- Consider purchasing insurance for Computer Fraud and Funds Transfer Fraud Transaction/Operations risk arises from fraud, processing errors, system disruptions, or other unanticipated events resulting in the institution's inability to deliver products or services. This risk exists in each product and service offered. The level of transaction risk is affected by the structure of the institution's processing environment, including the types of services offered and the complexity of the processes and supporting technology. Financial institutions should ensure their e-banking infrastructures contain sufficient capacity and redundancy to ensure reliable service availability.[12]

- Financial institutions should tailor their risk management and insurance strategies to the nature and complexity of their participation in retail payment systems, including any support they offer to clearing and settlement systems. Financial institutions must comply with federal and state laws

Common Questions to Ask an Insurance Provider

Firms should have an annual insurance policy review with their providers. Included below are some common questions to ask during those reviews:

1. Which perils are or are not covered under the current policy?
2. What insurance regulation changes are coming in the next year?
3. What increases in coverage should be considered?
4. What is the provider's biggest concern with current insurance coverage?
5. Are there any additional options?
6. Are there any incentives or benefits to financial institutions that have undertaken mitigation or continuity activities?

[12] http://ithandbook.ffiec.gov/it-booklets/e-banking/e-banking-risks/transactionoperations-risk.aspx

Questions Specific to the Financial Services Industry Cluster to Ask an Insurance Provider

The following questions are specific to the Financial Services Industry and should be asked during an annual (or more frequent if circumstances change) insurance policy review:

1. Can the provider insurance for Computer Fraud and Funds Transfer Fraud Transaction/Operations risk arises from fraud, processing errors, system disruptions, or other unforeseen events?

2. Can the institution's e-banking, e-insurance, or e-trading infrastructures be insured for loss due to disruption or malicious actions?

3. Is there available coverage for disruptions or theft from retail payment systems, including any support to clearing and settlement systems?

4. Can interdependence with payment system operators and third parties be insured in the event a disaster causes settlement disruptions that may cause unforeseen losses?

5. Is coverage or arbitrage available for liability due to disruptions to transactions (loan closings, issuance of policies, delays in executing market trades, etc.) due to system failures in the event of unforeseen hazards?

and regulations, as well as with operating rules of clearing houses and bankcard networks. From the initiation of a retail payment transaction to its settlement, financial institutions are exposed to certain risks. For individual retail payment transactions, risks resulting from compliance issues and potential operational failures including fraud are always present. Operational failures can increase costs, reduce earnings opportunities, and impair an institution's ability to reflect its financial condition accurately. Participation in retail payment systems may expose financial institutions to credit, liquidity, and operational risk, particularly during settlement activities. In addition, a financial institution's credit, liquidity, and operational risks may be interdependent with payment system operators and third parties.[13]

- Update policies for new equipment and facility upgrades, or new streams of revenue that are not currently itemized.

The National Flood Insurance Program (NFIP)[14] was created by Congress in response to increasing costs of floods, primarily due to disasters. At the time NFIP was enacted, flood insurance was not readily available or affordable through the private insurance market. Congress agreed to subsidize the cost of the insurance so premiums would be affordable. NFIP was recently changed, and the following links provide critical information on the program and those changes.

- Flood Insurance Issues in Recovery
- National Flood Insurance Program and Reforms
- National Flood Insurance Program
- Building Higher

[13] http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk-management.aspx

[14] http://www.fema.gov/national-flood-insurance-program