Industry Cluster Briefings Series

TECHNOLOGY CLUSTER

INSIDE

Overview

New Jersey's Information Technology sector can play a pivotal role in both comprehensive statewide recovery and long-term economic resiliency. The risks of a disruptive event such as a natural or man-made disaster causing significant physical and operational damage can be significant. It is important to invest in becoming resilient to these potential disruptions. The potential loss of innovations through loss of data and equipment may be catastrophic for technology-based firms. Specifically this cluster consists of the following types of businesses:[1]

- Information Technology
- Communication Technology
- Data Processing
- Hosting
- Other Gateway Services

Business Continuity Overview for the Technology 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[2].

Encouraging suppliers to demonstrate their continuity capabilities can also be a competitive requirement for future business – to provide more confidence in the suppliers' capacity to deliver on their orders. Integrating continuity planning up and down the supply chain can help identify efficiencies in "peace time" and build surety in production during disruption.

[1] http://www.state.nj.us/njbusiness/pdfs/industry/InfoTech.pdf

[2] http://www.usfa.fema.gov/pdf/efop/efo47103.pdf

Common risks and potential actions to reduce those risks for Technology companies are identified below:

Risk	Possible Protective Action
Lack of telecommunications, transportation, electricity, etc.	• Multiple redundant services and proximity of vendors to 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 worksite and alternative work locations
Telecommunications provider outage	• Consider using more than one provider, again in separate locations
Loss of communication with clients and staff	• In relying on several providers for cellular service and utilizing cloud technology, communication has a better chance of being maintained during a disaster
Security threat during disaster (human or malware)	• Either on-site or contractor-provided cyber security with specific disaster planning • Develop plans with local law enforcement and emergency management to maintain security during a prolonged absence. • Invest in remotely accessed security and surveillance equipment.
Loss of critical supplier capacity to complete orders	• Establish hard copy and electronic contact lists of primary and alternate suppliers (and competitors). • Establish contingency contracts with alternative suppliers.
Physical damage	• Develop contact lists of construction contractors, roofers, plumbers, landlords, building management etc. who can reliably respond to physical damage.
Disruption of customers operations	• Work with customers and suppliers to understand their continuity plans to appropriately set expectations for when and how those key links will be restored.

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 technology 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 Technology 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.[3] 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.

Suggested procedures for the Technology Industry Cluster:

1. Elevate Information Technology equipment storage
2. Establish redundant facilities
3. Establish a fail-safe phone system
4. Obtain a backup generator for critical equipment and operations

Summary of Suggested Data Management Solutions[4]

1. "Hot" Services:
   a. Real-time recovery, automated
   b. Clustered servers, both active and load balanced for better performance if one fails, partner assumes the entire load.
2. "Warm" Services:
   a. Low-Delay recovery, manual intervention
   b. Secondary server updated every few hours with snapshot of live data. Can reroute to this server if primary cluster fails.
3. "Cold" services:
   a. Longer delay recovery, high manual interventions
   b. Service contract with continuity vender can activate servers on shared server if need to resume from disaster.
   c. Off-site backup tapes, can be used to re-build server on new hardware after disaster.

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

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

[4] http://uwfemergency.org/documents/BCP_Slides.pdf

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 Technology Industry Cluster

Ensuring that a company is neither over insured nor underinsured is critical. Coverage must be designed in consultation with key personnel and legal counsel. Businesses can purchase bundled coverage, like the Commercial Package Policy (CPP). The CPP combines Commercial Liability and Commercial Property and some additional policies designed for specific industries. The Commercial Package Policy provides both property and liability coverage but has more flexibility to tailor the insurance coverage to the specific needs of a mid-sized to large business or a higher-hazard type of business. Technology Industry Cluster business may want to do the following:

- Insure property (including electronic records) of others that is in the businesses' care, custody and control to the extent that the company is legally liable for that property.
- Consider purchasing computer fraud and data loss coverage
- Consider additional coverage for electronic media if engaged in that business line
- Consider additional coverage for lost income and extra expenses in the event the ability to conduct e-commerce is slowed or stopped due to a computer virus or cyber-criminal attack.
- Consider additional coverage for compensating customers for credit monitoring in the event of an exfiltration of private or proprietary data.
- Update policies for new equipment and facility upgrades, or new streams of revenue which are not currently itemized.

It should also be noted business interruption caused by perils not covered by the base policy will most likely not be covered by a business interruption policy. For example if wind is not a covered peril, any business interruption caused by wind will not be covered. Check with the insurance provider on the possibility of covering specific perils covered by insurance.

The National Flood Insurance Program (NFIP)[5] 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

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 available to businesses that have undertaken mitigation or continuity activities?

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