A Law Firm's Competitive Edge: Writing Effective Business Continuity Plans

Presented by
Kathryn N. Scourby

LI15
5/3/2018
3:30 PM
A Law Firm’s Competitive Edge:
Writing Effective Business Continuity Plans
ALA Annual Education Conference – May 3, 2018

DEFINITION OF DISASTER OR CRISIS

“Any situation that threatens the integrity or reputation of a firm or business, usually brought on by adverse or negative media attention.”
DISASTER STATISTICS

50% (or more) of businesses that experience a major disaster will never return to the marketplace.

"By the time you hear the thunder, it is too late to build the ark." (Anonymous)

Of those that survive a major disaster, 50% (or more) will file bankruptcy within 3 years. (Chubb)

Those that survive are prepared to meet their clients’ needs by planning/preparing to react to a disaster.

Plan

2017 MAJOR CRISES

Active Shooter
Fort Lauderdale Airport
1/6/17

United Airlines passenger dragged off plane
Chicago O’Hare
4/9/17

Massive Power Outage
San Francisco, CA
4/9/17

Ariana Grande Concert Bombing
Manchester, UK
5/22/17

Civil Unrest
Charlottesville, VA
8/12/17

Hurricanes Harvey, Irma, Maria
Texas, Florida and PR
8/17 – 9/17

Equifax Cyber Breach
9/17

Las Vegas Strip Concert Shooting
10/1/17

Wild Fires
California Wine Country
10/17

Terror Attack on Bike Trail
NYC
10/30/17

Major Earthquake
Mexico City
9/19/17

Church Mass Shooting
Sutherland Springs, TX
11/5/17
OBJECTIVES OF SESSION

1. Why do Business Continuity Plans need to be written?
2. Determining the state of readiness of your Business Continuity plans
3. Determining whether you have all the necessary or required resources in place in your BC plan
4. Managing expectations of lawyers and staff in the event of a real disaster/emergency

REASONS FOR COMPREHENSIVE BC PLAN:

1. Compliance issues (Client audits, Outside Counsel guidelines and RFP’s)
2. Regulatory Requirements/Standards (government or ISO certification)
3. New Hardware, Data Security Systems or Applications in place for Cybersecurity
4. Facility and/or Personnel Changes/Moves/Relocation
5. Changes in Critical Third Party Vendor/Suppliers
6. Changes in Voice/Data Networks
ISO 22301 - standard that specifies security requirements for disaster recovery preparedness and business continuity management systems (BCMS).

ISO 27001 - formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information risks (called ‘information security risks’ in the standard).

ISO 27032 - provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: information security, network security, internet security and critical information infrastructure protection.

1. A DHS definition of Business Continuity “the ability of an organization to take a licking and keep on ticking”

2. Business Continuity plans are living, breathing documents

3. Maintenance and updating of plans is essential - plans should be updated on an ANNUAL basis (or more often when changes warrant)

4. Testing, Testing, Testing!!!
ESSENTIAL COMPONENTS:
WRITTEN BUSINESS CONTINUITY (RESILIENCY) PLAN

1. Incident Management/Risk Management Plan
2. Crisis Management and Communication Plan
3. Recovery Site Plan
4. Operational Recovery Plan
5. Information Technology (IT) Recovery Plan
6. Appendices

KNS Consulting, LLC

INCIDENT MANAGEMENT PLAN

1. Life Safety Procedures (Procedures for evacuation and Shelter-in-Place)
2. Key Contacts - Roles and Responsibilities
3. Emergency Operations Center Information (if needed)
4. Specific Documents and Data Needed
5. Damage Assessment Information
6. Restoration and Salvage
7. Insurance Considerations

KNS Consulting, LLC
RISK MANAGEMENT ISSUES

- Assess Risks (both internal and external)
- Security and Vulnerability Assessments
- Past Disaster Situations/Neighbor Disaster
- Geographic Locations
- Internal Systems or Processes Failures
- Supply Chain Risks

BUSINESS INTERRUPTION INSURANCE

1. Ensure firm/business has enough coverage if loss to physical property
2. Determine how to calculate losses/extra expenses incurred
3. Elimination period before coverage kicks in? Exclusions?
4. Consider purchasing cyber insurance

**Insurance does not cover the loss of clients**
CRISIS MANAGEMENT & Communication Plan

1. Identify Crisis Management Team
2. Procedures needed to transition from crisis to continuity of business operations
3. Ongoing communication with building management or landlord
4. All Notification procedures (including procedures for crisis communication systems)
   - Status Updates
   - Media Releases
   - All communications to interested parties

CRISIS MANAGEMENT TEAM

1. Consider size of office to determine how many members for team
2. Key admin players in the office
3. People who are willing to volunteer time
4. People who will be calm and authoritative in an emergency situation
5. Specific/separate crisis communication team
Consistent training for all Crisis Team members is essential

- Table Top Exercises
- Webinars
- Actual Drills
- Meetings
- Exercises
- Face-to-Face/On-Line Training

CRISIS COMMUNICATION SYSTEMS

1. Telephone Tree System
2. Toll-free number for all employees
3. Automated notification systems (reverse 911)
4. Password protected web page
5. Using Social Media
6. Test, Test, Test - update all systems frequently (Hawaii)
CRISIS COMMUNICATION

1. Critical Members of the Team
2. The Plan and How to Respond to a Crisis
3. Information for the Crisis Communication Kit

KNS Consulting, LLC

RECOVERY/ALTERNATE WORK SITE PLAN

1. Procedures for Alerting
2. Declaration of need to move to new location
3. Administration/Logistics
   - Alternate recovery location infrastructure (including options available to firm for relocation)
   - Determining need for new equipment
   - Determining need for other outside technical services

KNS Consulting, LLC
RECOVERY SITE
PLAN OPTIONS

- Work remotely from home
- Work from another office or location
- Temporary office facilities
- Contract with disaster recovery provider (mobile units or alternate facilities)

Ultimate goal: providing continuing service to clients

KNS Consulting, LLC

OPERATIONAL & TECHNOLOGY
RECOVERY PLANS

Procurement of any additional needed resources and data
- Vital Records
- Critical external contacts & suppliers (supply chain issues)
- Identification of key employees

Response time and recovery actions for functional departments (Business Impact Assessments) (BIA’s)

Prioritization structure for critical business functions (BIA’s)

KNS Consulting, LLC
1. Determine IT/DR recovery teams

2. Procedures for necessary resources: (Data location, data storage, voice and data communications hardware, all other hardware and software, key contacts and suppliers, equipment requirements, data backup information)

3. Redundancy is important as is knowledge of building IT/HVAC systems

4. Procedures for Cyber Security Protection

5. Procedures to redirect phone systems for ongoing communications

WRITTEN BC PLANS

- Well organized and easily communicated
- Lawyer/staff contact information
- Vendor/Business Partner contact information
- Checklist format (easy to use under stress)
- Items needing updating are easily accessible
- Links to other critical information (appendices)
- Consider an electronic version/app
TESTING OF BC PLANS

LEVELS OF TESTING – Documentation may be based on compliance or regulatory requirements.

1. Structured Walkthrough Testing (BIA’s)
2. Component Testing
3. Full Operations Testing

ABA GUIDELINES & RESOURCES

Committee on Disaster Response and Preparedness
www.americanbar.org/groups/committees/

Includes information:
A Lawyer’s Guide to Disaster Planning
Preparing Law Firms and Clients for Issues in Cyberspace

KNS Consulting, LLC
QUESTIONS?

KATHY SCOURBY, CBCP
KNS Consulting, LLC
(865) 789-7694
knscourby@gmail.com

Presentation may not be used or reproduced without permission – KNS Consulting
Your opinion matters!

Please take a moment now to complete the evaluation.

Thank You!