Legal and Backups

Legal requirements for backups

According to the American Management Association: “About 50% of businesses that suffer from a major disaster without a disaster recovery plan in place, never re-open for business.”

Fiduciary Responsibility

Fiduciary Responsibility is the responsibility that corporate officers have to investors.

”… the SEC has proposed a new Rule 206(4)-4, which would make it unlawful to provide advisory services to clients unless the RIA has a business continuity and transition plan (that is reviewed at least annually). In fact, the SEC has stated that it views having a business continuity plan as essential for an advisor to fulfill their fiduciary duty; or viewed another way, the firm that isn’t prepared for a business disruption isn’t prepared to fulfill its fiduciary duty to clients.” (Rule has been approved)

From: https://www.kitces.com/blog/sec-rule-2064-4-requiring-ria-business-continuity-plan-bcp-and-transition-plan/

Even though the rule has not been finalized the SEC expects companies to have robust business continuity plans in place as a part of fiduciary obligation.

Disruption can be in may forms. Floods, Fires, Earthquakes, Global Warming - or - just the death or disability of key personnel.

Legal responsibility due to contracts and SaaS

Two Parts

1. Who are your vendors - and do they have business continuity plans in place.
2. Who are your customers - do you have financial services companies, health companies, US or Foreign?

Backups fit into a “business continuity” Plan

1. Remember that business continuity includes -
    1. Loss of key personnel (because they quit, or ghost you)
    2. Death of personnel
    3. Natural Disaster (flood, earthquake, fire etc)

4. Non-Natural disaster - loss of power, network interruption (Back Hoe and Squirrels)

What will a plan include:

In each type of interruption, your plan should consist of:

- Step by Step process - list of contacts - list of responsibilities for each person
- Backup persons for each person
- Procedures that anticipate different scenarios

Short term / temporary interruption

How do you get a temporary interruption - internet failure, power loss, phone loss

Consider The Following:

- Backup and recovery of records
- Alternate means of communicating with customers - think backup website / backup email / SMS etc.

What happens when what seems to be a temporal interruption becomes a longer term problem?

Extended Interruption

How about when you have to relocate, replace systems, replace a primary vendor - or when you have malicious destruction of data or systems? Fire, Flood, Earthquake are also examples.

An extended interruption occurs when a firm has to relocate or replace office property or records due to destruction. An extended interruption could occur in the event of a fire, floor, or other natural disaster. Your firm’s BCP should address an extended interruption similar to a temporary interruption with a few additional considerations.

Consider The Following:

- Replacement of equipment - like serves - or vendors that provide servers
- Move of “owned” or “leased” equipment with virtual services (even if they cost more)
- Do your employees have the ability to work from home or from a remote location?
- Do your vendors have a business continuity plan?
- Can you connect to databases and servers from outside of the “office”?
- Do you have a reachability plan for all staph?

Permanent Interruption

Lots of forms of permanent interruption - but do be aware that fires kill 82% of small businesses (less than 500 employees) - Floods are just about as bad. Criminal fraud. Death or disability of key players in a business. Is a “succession” plan in place?

Consider The Following:

- Who will take over - who will data / IP be transferred to?
- Who will handle dissolution of the company?
- Backups of financial data are still required for 7 to 8 years - IRS 206 rule.
- Will clients be moved to some other service?

Legal Responsibility

Database Administrators face the very real risk include:

- Data Lost or compromised. This is probably the biggest item. The data is under the care of the DBA and now it is gone / messed up etc. If you combine this with SaaS the clients are in a position to sue. If the business is not carying Errors & Omissions Insurance the liability can be transferred to you. This is especially true if you have failed in your professional duties.
- Data Breach - the data is there but hackers have now. Protection of proprietary business information is part of the picture. Sensitive customer information, credit cards, passwords … is a 2nd part. Cyber Liability Insurance can help cover the financial fallout.
- Employee malfeasance. If any financial institutions are involved then a Fidelity Bond insurance should be purchased.
- Physical Theft. If servers get stolen then access to the systems has been compromised. Both Business Owner’s Policy and Liability Insurance are needed.

Public Corporations

In all industries

Regulation	Impact	Notes - Action Items
Sarbanes-Oxley Act	Corporate officers are liable for business continuity	Liability is only at the “officer” level in the company. Mandates business continuity and responsible planning includeing offside and accessible backups.
IRS Procedure 86-19	Requires off-site protection and documentation of computer records relating to tax	Records must be available in the event that the primary facility is subjected to unplanned outage

Regulation	Impact	Notes - Action Items
Consumer Credit Protection Act (CCPA) Section 2001 Title 1X	Due diligence for availability of data in Electronic Funds Transfers including Point of Sale	Requires offside access to data
Foreign Corrupt Practices Act 1977	Publicly held corporations must provide “reasonable protection” for IT systems	Holds all “management” accountable including computer system administration.

Healthcare Specific

Regulation	Impact	Notes - Action Items
Health Insurance Portability & Accountability Act (HIPAA 1996)	Requires data back-up plan, disaster recovery emergency plan, and emergency mode operations plans	DBA’s , Developers, IT held personally responsible. Liability includes prison terms. Auditing required.
Food and Drug Administration (FDA) Code of Federal Regulations (CFR), title XXI, 1999	Requires Business Continuity measures to ensure availability of information Establishes the requirements for electronic records and electronic signatures	Devs and IT personally responsible. Remote access to databases/systems during emergencies is required.

Government

Regulation	Impact	Notes - Action Items
Continuity of Operations (COOP) and continuity of Government (COG)	Federal Preparedness	Establishes requirements for Business Continuity plans and response readiness. Includes any non-federal that receives funds from federal.
	“Business Continuity plans must be able to sustain operations for 30 days	This includes remote access to systems and remote systems.
	All Business Continuity plans must be maintained at a high level of	
	readiness, must be capable of implementation without	
	warning, must be operational within 12 hours…”	

Regulation	Impact	Notes - Action Items
FEMA FRPG 01-94	All department and agency heads must formally plan for continuity of essential operations	This includes yearly testing of recovery procedures (restore backups)
	Written documents for Business Continuity must be maintained and current	
Federal Information Security Management Act (FISMA) 2002	Requires electronic data to be available during a crisis Emphasis of FISMA is on data security	
National Institute of Standards and Technology (NIST) SP800-34 2002	Requires electronic data to be available during a crisis Emphasis of FISMA is on data security	
National Institute of Standards and Technology (NIST) SP800-34 2002	Requires Business Continuity/Disaster Recovery and COOP plans	
NIST 800-53 2005	Recommended security controls for Federal Information systems	Mandatory security controls with specific requirements for continuity planning (remote access to , availability of computer systems)
Governmental Accounting Standards Board (GASB) Statement No. 34 1999	Requires a Business Continuity plan to ensure that agency’s mission continues in time of crisis	

Applies to all government entities that operate utilities Utilities North American

Regulation	Impact	Notes - Action Items
Electric Reliability Council (NERC) P6T3	Interim provisions required if it takes in excess of 1 hour to implement primary facilities Business Continuity/Disaster Recovery Plan	Specific details on Business Continuity/Disaster Recovery plan that include communications, monitoring utilities, training and testing
NERC Urgent Action Standard 1216	Disaster Recovery Plans and procedures must be in place	Business Continuity plans are only required for facilities and functions considered “critical.”

Regulation	Impact	Notes - Action Items
Federal Energy Regulatory Commission (FERC) RM01-12-00 2003	Mandatory Recovery Plans Does not apply to rural utilities service borrowers and limited distribution co-ops	
NERC Security Guidelines for electricity sector 2001	Includes Business Continuity/Disaster Recovery in information security standards for the	
industry-government partnership		
Guided by Critical Infrastructure Protection Committee (CIPC)	Plan required for rural utilities	Condition of continued borrowing for rural utilities services
RUS 7 CFR Part 1730 Emergency Restoration	Plan required for rural utilities	Condition of continued borrowing for rural utilities services
Presidential Decision Directive 63	Encourage risk management strategies to protect	Applies to interdependent and cyber-supported infrastructures vulnerabilities in both public and private
	against and mitigate effects of attacks against critical infrastructures and key resources	sectors, to protect both domestic and international security.
Presidential decision directive 13010	Disaster Recovery plans required for all national infrastructures	
FTC’s Federal Information Security Management Act 16-CFR-314 2003	Addresses incident Management response and reporting and Business Continuity/Disaster Recovery planning	Focus is on security issues, such as password management.
TL9000 Section 7.1.C.3	Requires established and maintained Business Continuity/Disaster Recovery plans “to ensure the organizations ability to recreate and service the product throughout its life cycle.”	

Normal tests for Backup / Continuity

- Annual tests of backup plan
- Test for different types of disruption
- Verify availability of backup equipment
- Have both electronic and written(printed) versions of action plan
- Very that critical employees have copies of the plan