InfoSystems Integrated

FAIL SAFE Contingency Planning

Five Rules to Stake Your Plan On

1. Plan to fail

Most plans are too optimistic. When things go awry, they typically go from bad to worse -- rapidly. Planning to fail means envisioning and detailing potential failure scenarios and documenting your contingency plan for each situation.

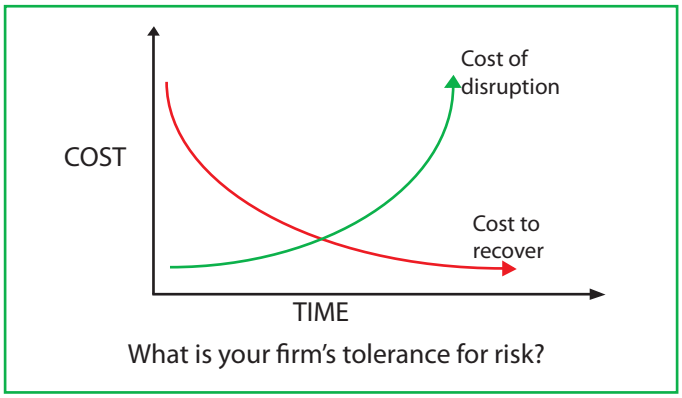
For example, we recommend three forms of backup (with the assumption that one or two of the backups may not be sufficient). While many of the firms we work with could probably get away with a single backup method, each method that we implement lowers the overall risk of losing any data.

2. Don't set it and forget it

Remember, there is no silver bullet. The day you don't check your systems is the day you should expect them not to work. Systems are ultimately managed by people and even the most competent people sometimes make mistakes. Beware of vendors that tell you, "It's automatic. You don't have to do anything."

If you have a metered Internet backup service and you are getting billed monthly, the invoice amount should never be the same. If it is, it may indicate that the data being backed up isn't changing.

Absolute vigilance is required to be successful at planning for a contingency.



What is your firm's tolerance for risk?

3. Establish strict and coherent responsibilities

Who is the steward of your firm's plan? How do they validate the plan? How does the plan work? Our real-world experience indicates that multiple parties need to understand and check the plan for problems on an ongoing basis. When new systems are implemented a disciplined approach to adding and updating the contingency plan needs to be executed.

4. Institute operational checks and balances

We recommend a multi-faceted approach designed to ensure that multiple parties independently share ultimate responsibility for backing up your company's data and validating that the contingency plan works. Your firm cannot afford to make assumptions about whether those responsibilities are being met.

If you think you're ready, test it. Ask your IT folks to throw the switch with little or no warning to see how well your plan really works. You may want to think about this carefully since some plans are like having a gun that can only shoot one bullet. In order to test the system again you may need to rebuild the system.

5. Continuously improve and refine

Contingency plans fall into five basic categories: non-existent, poor, okay, good and excellent. As a decision maker and responsible party at your firm, do you know how your firm's plan would rate? Moreover, IT systems are in a nearly constant state of change. If your plan was "good" last year, is it as "good" today?

A company that has an excellent contingency plan for a catastrophic event may not have a good plan for the more likely event of losing Internet access at their office tomorrow.

There is always room to improve your plan.

InfoSystems Integrated : www.isitc.com : sales@isitc.com : 617.720.3400

Five Rules to Stake Your Plan On (continued...)

Evaluate Your Firm's Contingency Plan					
Plan Rating	Nonexistent	Poor	Okay	Good	Excellent
Preparedness	Backup only	Own a backup server	Co-located facility where systems reside	Ability to restore systems manually on a regular basis	Automated synchronization or equivalent on a daily basis
Philosophy	"I can't imagine I'd ever need to, but I'm confident that everything will be restored with the tape."	"I assume my IT folks will drop everything else to get my firm going again if there is a disaster."	"I've established a site to house my equipment and realize that I still need to have a more robust plan."	"I realize that it's going to take time to restore my data, but I'm prepared to make do without all of my systems for a couple of business days."	"My firm made a substantial investment to ensure that my systems are up and running ASAP, but I know the switch will take time to implement."
Recovery Time	1-2 weeks	1 week	3-4 days	1-2 days	2-4 hours
Stage	Denial	Acceptance	Planning	Implementing	Validation
Cost	$	$$	$$$	$$$$	$$$$$

Fail-Safe Services:

Contingency Planning
With our experience helping financial services companies prepare their IT contingency plans, we can help fast track your company's written contingency plan.

Assessment and Validation
Our knowledge of the industry and its particular requirements places us in a uniquely qualified position to evaluate existing plans. Assessments can be done at a surface level to validate the infrastructure, or at a more detailed level to audit actual functionality.

Data Vaulting
Working with our Internet backup provider, we can arrange for primary or secondary Internet backups of your critical data to be performed. This data is stored in encrypted form so your data is secure.

Server Hosting
ISI has partnered with one of New England's top providers of co-located secure data center environments. Ask us for a quote based on your hosting requirements.

InfoSystems Integrated : www.isitc.com : sales@isitc.com : 617.720.3400