

Business Resiliency Planning for the Mobile Workforce

How To Guide

Addressing business continuity, information security,
policy enforcement, and regulatory compliance
for your mobile workforce

By Datacastle
January 2010

Contents

Executive Summary	1
Business Resiliency Planning Process	2-7
- Analysis	2
- Solution Design	5
- Implementation	5
- Test & Maintenance	7
Mobile Workforce Resilience: Datacastle RED	7

"Business Resilience is a lifestyle that an organization embraces to ensure that it can thrive in the face of the unexpected while meeting regulatory compliance."

Executive Summary

How do organizations keep their mobile workforce productive while safeguarding critical business information? IT organizations are staring down what can be an overwhelming set of challenges – less tolerance for “downtime”, exploding data growth, an increasingly mobile workforce, and more demanding regulatory compliance requirements. Critical business information no longer resides solely in protected data centers, but is increasingly found on laptops, opening up a new set of vulnerabilities that must be addressed. Just as there was a maturing transformation from Disaster Recovery (DR) to Business Continuity Management (BCM) over the past decade, there is now a recognition that we must progress from BCM to the concept of Business Resilience.

Business Resilience is a lifestyle that an organization embraces to ensure that it can thrive in the face of the unexpected while meeting regulatory compliance. Traditional BCM focused on dealing with potential major disasters, including how your organization would recover from such an event. Business Resilience means that your organization is prepared to deal with large disasters (e.g. flood, fire, riots, earthquake, war, etc...), mid-sized incidents (e.g. lost or stolen laptop) and small accidents (e.g. corrupted file, accidentally deleted file). Business Resilience means that you can protect your critical business information from security threats and meet compliance mandates (e.g. HIPAA, SOX, GLBA, PCI, etc...) without negatively impacting the productivity of your workers.

What follows is a framework for developing a business resilience plan for your organization. There are many considerations to take into account because of the multi-faceted nature of the challenge. There is no “silver bullet” that will solve the business resilience challenge facing your mobile workforce, but implementing best practices and policies can lead to competitive advantage, real bottom-line savings and perhaps most importantly protecting your reputation.



There are many considerations to take into account when solving the business resilience challenge facing your mobile workforce

"Telecommuters, managers who take their laptops home in the evenings or weekends, contractors – all of these workers leave the office with valuable business information on their laptops..."

The Business Resiliency Planning Process

The Business Resiliency Planning process is broken down into 4 phases:

- Analysis
- Solution Design
- Implementation
- Test & Maintenance

Analysis

The analysis phase will enable you to determine if you have an effective business resiliency solution for your mobile workforce. The following deliverables are produced during this phase:

- Business Impact Analysis
- Threat Analysis
- Regulatory Compliance Analysis
- Recovery and Protection Requirements

Business Impact Analysis (BIA)

If you have conducted a Business Impact Analysis for core IT systems in the past, this is a similar process with a few twists.

Define your "Mobile Workforce"

The first step is to determine who makes up your mobile workforce. It's obvious to include sales professionals, accountants, HR professionals and IT personnel that travel on a regular basis. But what about other employees with laptops that leave the office? Telecommuters, managers who take their laptops home in the evenings or weekends, contractors—all of these workers leave the office with valuable business information on their laptops, making it critical to include them in your plan.

Inventory and Categorize Business Information

Once you have defined your mobile workforce (and it is likely larger than you may have originally thought), it is important to understand what information these employees need to perform their job function and what is travelling around on their laptops or sitting on remote desktops. For example, health care professionals providing care in the field may have patient records. Sales people will have customer information. Insurance agents will have customer records and policy quotes. Consultants may have confidential customer information. Telecommuting HR professionals may have employee records, performance reviews, employment contracts, and more.

Once you have taken an inventory of the business information that your mobile workforce has access to, it is important to characterize the information. Not all business information is equal, requiring the same level of protection. Some information is necessary to perform a job function; some information is proprietary and constitutes critical trade secrets. While your characterization can have many categories, it is recommended that you should at least use "Critical" and "Non-Critical".

From this inventory of information assets needed by your mobile workforce, you can make a determination of "Critical" asset recovery requirements by considering:

- Recovery Point Objective (RPO) – the tolerable period of information loss
- Recovery Time Objective (RTO) – the tolerable period to recover the information
- Recovery Device Objective (RDO) – the location and device targeted for information recovery

For most business continuity professionals, RTO's and RPO's are commonplace. However, for a mobile workforce the target device for information recovery may vary depending upon the nature of the incident and the location of the mobile employee.

Be sure to take into consideration the economic impact of not meeting these requirements. For example, if your organization has a data breach that requires a public notification, not only is the organization subject to fines for the relevant regulator, but you can also expect to lose some customer relationships over the incident or generate negative press coverage which can have a broader economic impact.

"Threats can come in all sorts of shapes and sizes. "

Threat Analysis

Threats can come in all sorts of shapes and sizes. Their level of impact on the organization varies as well. Ideally, you want to design a single solution framework to address the spectrum of threats. For each category of threat, you should determine the scope of the threat and the economic impact. When it comes to performing this for the mobile workforce, it is important to perform a dependency analysis. For example, if a member of your executive team loses their laptop, the scope of the impact isn't just limited to the hours of productivity lost to the executive. Depending upon the sensitivity of the information on the laptop, other impacts may include data breach implications, potential customer loss due to sensitive information being exposed, and the hours of productivity that the rest of the organization will lose conducting an audit trail and dealing with the fallout of the laptop loss.

Large Disasters

These are classic disaster recovery incidents such as floods, fires and earthquakes. Organizations have been better at determining risk associated with centralized IT assets (e.g. data centers, servers, etc...), but have not done as well when thinking about their mobile workforce. For example, during Hurricane Katrina, the mobile workforces of many companies were in position to be much more responsive, but many information assets were lost or compromised because home computers and laptops were destroyed in the disaster. With a mobile workforce it is essential to understand the impact of new threats such as pandemics and how an organization can respond when their mobile workforce is impacted.

"...business resilience means keeping your workforce productive in the face of a spectrum of negative events."

Mid-Sized Incidents

Losing a laptop or having a laptop go stolen is an everyday occurrence. Such events are no longer isolated to the productivity of a single employee. Because more sensitive information has been making its way to remote offices and onto the laptops of mobile workers, it is now critical to include these devices as part of a robust data protection plan. This includes the ability to encrypt information at rest, to automatically back up the device without user involvement, and to remotely shred information if a laptop is lost or stolen.

Small Accidents

Small accidents are often overlooked in a business continuity and disaster recovery plan. However, business resilience means keeping your workforce productive in the face of a spectrum of negative events. Accidental file deletion and corruption are daily occurrences. You need a plan in place to enforce backups, without relying on end users or interfering with their productivity.

Regulatory Compliance Analysis

The next analysis that needs to be performed is whether or not there are applicable regulations that require the business information held by your mobile workforce to be protected in specific ways or not. For example, if your company is in healthcare or pharmaceuticals, you can rest assured that HIPAA applies to you. If you are in the financial services industry or retail, you must meet PCI mandates. SOX compliance is a requirement for public companies. If you have customers in the state of Massachusetts, you can expect to comply with 201 CMR 17.00. Be aware that other states are currently evaluating similar legislation.

Recovery and Protection Requirements

At the conclusion of performing the Business Impact Analysis and the Regulatory Compliance Analysis, you are in excellent shape to pull together your final requirements. The recovery and protection requirements will impact your solution design approach. Your requirements should be the summary of business continuity requirements (e.g. RTO's, RPO's, RDO's), your information security requirements (e.g. access, permissions, etc...), and your regulatory compliance requirements (e.g. encryption requirements, data destruction requirements, etc...).

The final step in this phase is to prioritize these requirements by taking into account their likelihood to occur, potential economic impact, and regulatory mandates. Once you have pulled this information together, you can now proceed to the solution design phase.

"Especially when it comes to regulatory requirements, creating dependency on end user behavior is the surest way to end up out of compliance."

Solution Design

Consider the following when developing your solution design:

- People
- Policy
- Systems
- Enforcement

Be sure to follow these guidelines when designing a business resilience solution for your mobile workforce:

Stay out of the way: The whole reason you are putting a business resiliency solution in place is to make your mobile workforce more productive in the face of the unexpected. Don't create policies and implement systems that inhibit the day to day productivity of the employees that you are trying to make more resilient. The less "visible" the solution, the more likely it will be adopted and used.

Less dependence on end user behavior is best: Many IT departments will address their business resilience challenges by rolling out policies that are dependent on end user behavior. Especially when it comes to regulatory requirements, creating dependency on end user behavior is the surest way to end up out of compliance.

Keep it simple: If your solution is going to require many nuanced policies, multiple vendor solutions, and multiple agents on the employees laptop, then you are increasing your execution risk. Keep policies as simple as possible and try to consolidate your technical solution into as few vendors and agents on the laptop as possible. Your likelihood for success will go up dramatically.

Prioritize: Target the mobile workforce that possesses the greatest risk to the business. More often than not, this starts in the executive suite where the management team is flying around with unprotected laptops that have timely and sensitive business information.

Plan to scale: You should assume that once you start implementing business resilience for one job function, that success will necessitate the demand to roll it out to other job functions. Identify a solution that can be replicated in multiple job functions and span the organization.

Implementation

Goals, people, and process are the key elements to a successful implementation.

Goals

The goals of your implementation should be clear, simple, measurable, and fully supported by both management and the execution team. A typical goal would be to roll out the capability to a particular user community within a set of constraints such as a time period and budget.

People

As a result of the previous phases, you should have an excellent idea of the requirements and stakeholders for the implementation. Make sure there is clear leadership for the project and that those affected understand its importance. Make sure the team has the resources needed and the scope of control to make the implementation successful.

"It is key that your mobile workforce resilience implementation integrates well with reporting and audit processes that exist within your compliance management function."

Process

There are critical processes that need to be managed by the implementation team. The processes you should focus on are:

Project management

This is the day to day management of the implementation to make sure that the identified tasks are getting accomplished on schedule, and that the necessary resources are in place to make the implementation successful.

Risk management

As with any project, it is important that the implementation team periodically reviews internal and external threats to the success of the implementation. Understanding the scope and severity of such threats, and determining what (if any) mitigation strategies will be used to reduce the risks to the implementation effort, will help keep the project on track. A common risk management challenge is the interdependencies with resources outside of the core implementation team. Such interdependencies should be kept to a minimum.

Communication management

The implementation team can be so heads down on the tasks of the day that they can often overlook the critical role that communication plays within and outside of the team. It is important to remember that the beneficiaries of the effort are the mobile workforce and the organization's management team. Make sure that key milestones are communicated effectively, that the benefits of the program are communicated to all stakeholders and that if there are changes required by stakeholders, that such changes (e.g. change in policy) are promulgated effectively.

Compliance management

Organizations that are in regulated industries often have a compliance management function within their operations. It is key that your mobile workforce resilience implementation integrates well with reporting and audit processes that exist within your compliance management function. For example, rolling out the key policies surrounding at rest encryption and data destruction policies are just the beginning. Change control, enforcement, and audit/reporting must also be addressed to reap the benefits and mitigate compliance risk on an ongoing basis.

Test and Maintenance

After successfully rolling out your mobile workforce resilience plan, it is important that you regularly test the systems in place to ensure that they work as expected and corrective actions can be taken in the event that they do not.

"...design tests that will determine if recovery time objectives (RTO's), recovery point objectives (RPO's), and recovery device objectives (RDO's) are being achieved."

It is recommended that such tests should be conducted twice a year. Remember that the purpose of the workforce resilience effort is to keep your mobile employees productive in the face of large disasters and small accidents. As a result, you should conduct the tests in such a way that is not disruptive to the productive hours of the workforce.

When approaching tests, you should return to your requirements and design tests that will determine if recovery time objectives (RTO's), recovery point objectives (RPO's), and recovery device objectives (RDO's) are being achieved. Try to design the tests to be as pass/fail as possible to minimize debate about the results of the test. In the event of a failure to achieve one of the requirements, the team should conduct a root cause analysis to determine the cause of the failure and come forward with a set of recommendations that can mitigate or resolve it.

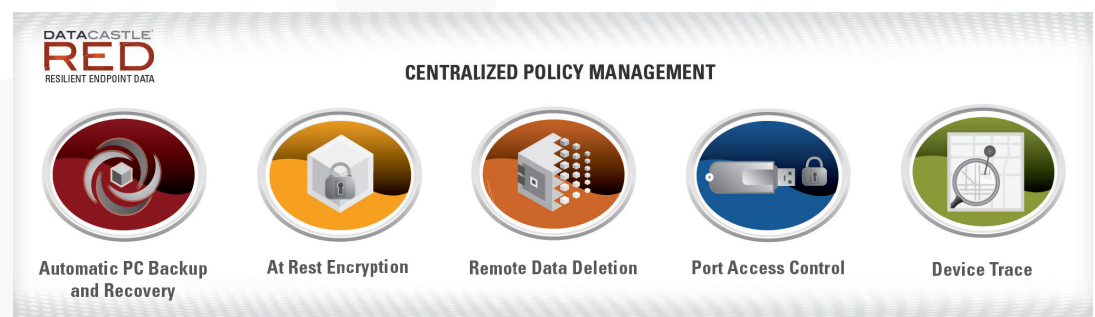
By conducting a test and maintenance cycle at least twice a year, you can rest assured that your workforce resilience systems are operating within expected parameters and will provide the benefits you seek.

Mobile Workforce Resilience: Datacastle RED

The complex set of challenges that need to be met with a mobile workforce resilience plan is the mission of Datacastle RED.

One product does it all—Encrypt. Recover. Delete.

- Keep it your business: state-of-the-art encryption protects files at rest, during backup and recovery.
- Backups that happen without relying on or bugging your users: less worry and less grief— isn't that nice!
- Turn off unauthorized data leakage with built-in port access control.
- Shred sensitive information for good on your command—now that's power!
- Get back to work fast: let trusted users easily recover their own files without calling IT.
- Disgruntled employees think twice about swiping traceable laptops, and you have a fighting chance of getting missing assets back.



Learn More

To learn more about Datacastle RED, please visit our website at www.datacastlecorp.com, email us at info@datacastlecorp.com, or call us at (425) 996-9684.

About Datacastle

Datacastle makes an organization's mobile workforce resilient to the unexpected. Listed in Gartner's Hype Cycle for Storage Technologies, 2009, Datacastle RED turns vulnerable business information into a resilient, managed business asset. Datacastle empowers IT to enforce data policies and exceed compliance requirements. For more information, visit <http://www.datacastlecorp.com>.