

Business Continuity, Disaster Preparedness & Recovery Support for SMB's

Business Continuity and Disaster Recovery in Volatile Situation

Characteristics of a Disaster

- Disasters are very fluid and require quick deployment and mobility during and after event
- Officials and experts will likely not know how long the emergency could last.
- Local resources will likely be unavailable for long periods of time – power, communications resources, etc.
- Workers may be unable or unwilling to travel to their jobs and choose to work remotely.
- Local authority will likely be stretched beyond capacity – remotely managed, credential-based access to information is critical.
- Communities may be affected in waves that last for months and even years.
- State and federal laws may be modified, suspended or enacted in response to an emergency.
- Social and economic disruption is likely.
- Cyber-Thieves will use this time to step up attacks.

RocITSafe™ - Bare-Metal-Boot Virtual System on a Stick is designed from the ground up to provide one of the most secure virtual USB computing platforms ever constructed – the ultimate in secure mobile computing. RocITSafe leverages virtually any PC-based laptop or desktop computer system as the host platform. Then it seamlessly incorporates device management within the RocITSafe guest operating system, supports industry standard software packages and proprietary packages that run within the RocITSafe guest operating system(s) (Windows XP; Windows 7) providing users the flexibility to customize their individual RocITSafe platform according to specific needs or desires without compromising security and data protection within the RocITSafe computing system. RocITSafe supports everyone from the casual user to the sophisticated Super-user.

Problem Statement

For small and medium-sized businesses (SMBs), the impacts of a disaster can result in loss of or lack of access to data, applications, and work facilities. Hurricane Katrina's devastation of the U.S. Gulf Coast in 2005 impacted countless businesses, from retail stores and hotels to major corporations. Those with disaster recovery plans in place fared much better than those without such contingency plans.

More SMB's Beginning to Plan for Disasters

While the business impacts of disasters – such as the loss of data and communications infrastructure, leaving a business unable to function – are widely understood, SMB have been slower to develop disaster recovery plans as compared to larger organizations. But that appears to be changing. According to the Yankee Group's U.S. Small and Medium Business IT Survey, after security the other major concerns of SMBs are now backup and restore and then application and data availability. Globally, spending on data protection and recovery management among all businesses will surge from \$58 million in 2006 to more than \$200 million by 2011, according to research from IDC.

Yankee Group analyst Gary Chen found that among SMBs, "Most are on the edge, where a couple of bad events could shut down business. They need regular backup, either traditional scheduled file-based or continuous. And they need to have it off-site and tested, to ensure they can bring up critical applications and data if headquarters is wiped out."

People, processes, training, and planning are also part of effective disaster preparedness. Here are five key steps to consider when implementing a program for your company.

1) Understand what data and systems are critical to business continuity

Many governments have mandated the remote replication and storage of financial, medical, and certain other kinds of data. Businesses have realized that their data and applications are their life blood. Make sure you know where all of your company's critical data and applications are located and that they can be integrated into a remote backup solution.

2) Identify and fix single points of failure in your network, business processes, and people

In network design, redundancy eliminates single points of failure. Make sure that network elements – including switches, routers, and other components – are redundant and enabled with software failover features. Review business processes and job responsibilities to ensure that there are similar "failover" mechanisms in place should a process or employee become adversely affected in a disaster.

3) Create a workforce continuity plan

If employees can't get to their offices for days, weeks, or longer, it is important to understand what kinds of remote access solutions they need to continue being productive, based on their individual job requirements. For example: Back office workers need access to applications and data and can probably use e-mail or instant messaging to communicate.

Other categories of employees whose jobs require a lot of collaboration may need high-availability voice-over-IP (VoIP) services along with access to corporate data and applications. The benefit of IP and Ethernet in a disaster is that they are so pervasive compared to other technologies that devices are truly plug and play.

Executives and employees who must interact with customers, partners, or the press may need remote communications solutions with guaranteed quality of service (QoS), a VoIP phone with guaranteed toll-quality service, and collaborative software applications which allows audio and video conferencing.

4) Create a disaster recovery plan

A formal plan should be initiated and endorsed by senior management and should involve all levels of personnel in your company. An inclusive process of gathering information and drafting the plan will create the necessary sense of everyone's ownership in and responsibility for disaster recovery.

5) Train your staff on disaster response

Training and practicing facilities evacuation and other emergency responsibilities for certain types of disasters relevant to your business could have dramatic consequences related to personnel safety, business continuity, data confidentiality, and asset security in the event of a real disaster.

Specifically, when considering the technological challenges that must be addressed during a disaster, it becomes quite clear that it is exactly these types of events – during the time when people, businesses and government agencies are at their highest risk – provide the greatest opportunities for cyber-thieves and cyber-terrorists to hit the hardest.

RocITSafe™ - complete data protection on Ultra-mobile platforms

RocITSafe is available today on multiple sizes of FIPS and non-FIPS certified thumb drives as well as FIPS and non-FIPS certified USB spinning hard drives in sizes to over 500GB. RocITSafe creates a highly secure and ultra-mobile container in which the user environment resides including a user-specified OS, user-specific application software, device management tools and Anti-Virus software as well as user-generated data.

Disaster Recovery Plan Should Include:

- Risk and threat analysis
- Leadership and succession plan
- Emergency response plan
- Internal and external communications requirements
- Human resources responsibilities
- Facilities management
- Availability of information and communications technology
- Cooperation with first responders, public officials, vendors, partners, and customers

Solution Brief: Disaster Recovery Support

By adding CAC/PIV/Smartcard fully integrated login support within RocITSafe, the system has multi-factor authentication, which virtually guarantees your system cannot be compromised through unauthorized access and because of the unique design characteristics of the RocITSafe stack, outside unauthorized access points into the system are eliminated.

Real Threat – Real Solution

In this worldwide heterogeneous technological environment more data is transmitted in a single hour than the sum total of the entire Library of Congress and then some – a severely under protected network and mobile environment where people are lulled into the misplaced belief that their information is safe and secure. Add to this, that workforces will overnight become remote workers scattered and working in uncontrolled settings that usually are not considered, the result can be devastating.

Business Continuity (BC) and Disaster Recovery (DR) are critical components of any SMB plan. With workers scattered remotely both control and support are at best minimal. Yet at these critical times, maintaining continuity and recovery of operations within the organization is vitally important to the long term recoverability after the emergency subsides. Failing to provide support in these two areas can result in loss of important data, loss of productivity and possibly loss of revenue and even disastrous longer-term impact on the organization such as total business failure. A recent statistic quotes 50% of those businesses that suffer major data breaches, data losses due to catastrophic emergencies and organizations that do not have BC and DR plans in place fail within 5 years after the occurrence of such event.



Social distancing (SD), self-shielding, voluntary isolation, and reverse quarantine are all methods that attempt to limit close physical proximity between infected and healthy individuals. They provide individuals with some measure of personal control over their own exposure to a potential emergency. SD can be instituted voluntarily by individuals or through actions taken by local, state, or government officials such as closure of public office buildings, schools, discontinuance of public transportation, and restrictions on large gatherings or public venues. Additionally, businesses with a BC/DR support plan may institute an (SD) policy for their workforce during a major disaster. All of these have significant impact on the community and workforce.

Disaster Support Solution

RocITSafe combines technologies to provide a standardized method to secure information on Ultra-mobile devices – technology that allows the information to protect itself. RocITSafe technology is highly portable and standards based so can comply with local, state, federal and international data protection standards as they are adopted around the country and around the globe.

The software stack is designed to provide a high degree of flexibility in configuring the systems according to specific user requirements. Specific policies governing Disaster Recovery and Business Continuity within the organization can be included, managed and enforced within the RocITSafe stack.

RocITSafe supports standard methods for connecting to the network including landlines, basic WiFi, WiMax, Mobile Intelligent MiFi hubs, VPN access and others to supports Social Distancing while maintaining smaller functional coherent workgroups which allow the users to lock down an open Internet connection, create a highly mobile and secure endpoint to safely connect to critical resources and use a uniform tool set that is easily maintained by small IT organizations before, during and after a major catastrophic event.

Mobile workers and/or students can connect to the secure RocITSafe solution using their ID Cards and a portable CAC/PIV or Smart Card Reader.



About RocITSafe Family: Securing, Enabling, Mobilizing

The RocITSafe bare-metal-boot (BMB) solutions are best suited to companies that want to virtualize the entire user's desktop, while RocITSafe Pluggable (PG) is better suited to deploying certain applications that the users need all the time, such as a VPN connection or certain desktop applications. PG collaborates with the operating system on the PC, while BMB runs with its own standalone highly secure operating system.

Under central administrative control, both versions can restrict what executables can run within the virtual desktop, and thus prevent data leakage via malware on the host PC.

Absolute Identification's RocITSafe family of products are designed and developed from the core with the highest level of security in mind. Every RocITSafe solution contains a fully integrated and highly secure operating environment that dramatically enhances the ability to protect the user against Cyber-theft.

Headquarters

5353 Scotts Valley Dr.
Suite D
Scotts Valley, CA 95066
Phone: (831)459-8199
Toll Free: (888)459-8199
Fax: (831)480-5886
Info@absolute-id.com

ABID International

114 France St.
DDO, Quebec
Canada, H9A 1K1
Phone: (831)278-0957
Fax: (831)515-5256
Canada@absolute-id.com

ABID Federal

22 East 35th Place
Steger, IL 60475
Phone: (708)755-1583
Phone: (831)278-0952
Fax: (831)515-5215
Federal@absolute-id.com