



Workplace Recovery and the Secure Pocket Drive

How Secure Pocket Drive Can Ease The Move to a Recovery Center

Introduction

True business continuity means keeping your business running. If your people cannot get back to work and be productive after a disaster, all of the resources that you expended to protect your data centers and keep them running was a waste of money. Companies can contract with SunGard, Rentsys, IBM, HP, or a handful of other companies to either use space in a fixed facility or to have a trailer driven or airlifted to a convenient location. However, there is extensive preparation required by your vendor and your company when your contract is first signed, and again after you have declared a disaster and need to move in to a workspace recovery unit. This paper discusses those preparations and how Secure Pocket Drive from SPYRUS can make your move to a recovery center a whole lot easier.

Like Chinese Food

You go into a Chinese restaurant and order from the menu. A few minutes later, your food shows up. Looks easy, right? What you don't know is that well before the restaurant opened and all through the day, there is a substantial amount of prep work going

on behind the scenes. Unlike a steak restaurant where you cut your meat and vegetables into bite-sized chunks at the table, hundreds of pounds of meat and vegetables need to be cleaned and chopped or diced in preparation for being tossed into the wok for cooking.

Similarly, there is a substantial amount of prep work that needs to be done before you can move into a workplace recovery center. After you sign your contract, you and your vendor will work together to develop the infrastructure your company needs to get your employees back to work. One of the first steps includes building and configuring the infrastructure to connect to your backup data center (which may be self-hosted or hosted by the same or a different recovery vendor). Unless your network or server configuration changes dramatically, maintenance is fairly easy.

Endpoint Preparation

One of the more involved aspects of workplace recovery is configuring your endpoints. In plain English, this means setting up the PCs that your workers will actually be using in the recovery



center. The prep work involved in setting up your PCs is extensive and ongoing. The “gold master” (GM) configuration that you use for your desktops and laptops is a good starting point, but you might be using Dell PCs while your workforce continuity provider might supply Lenovo or HP computers. This means that in addition to testing your GM on your own computers, you also need to test it on the provider’s computers as well. And you can’t just stop there and burn a GM CD, because Microsoft and Adobe are constantly releasing patches to fix bugs and close zero-day exploits. So whenever you patch your internal computers, you need to run the same tests on your provider’s computers and create a new GM.

Well I Declare!

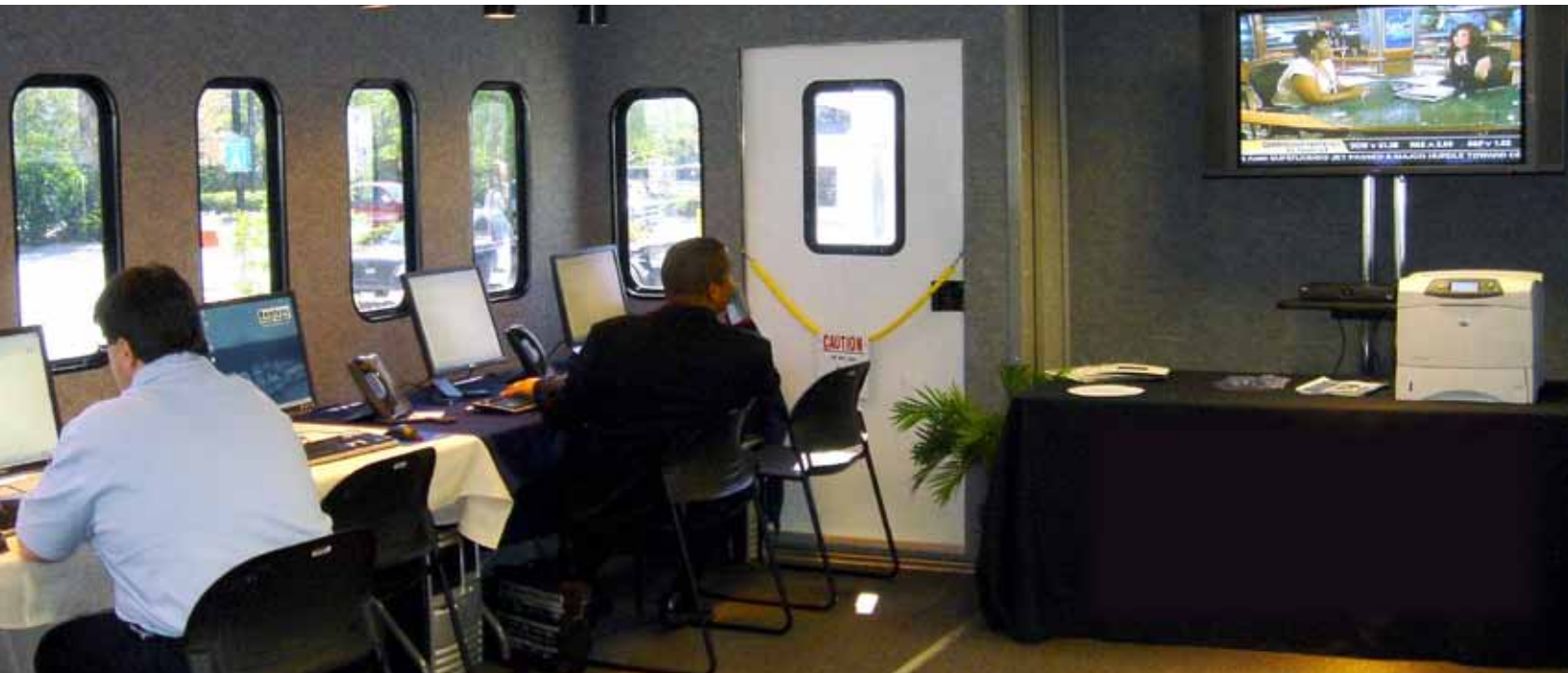
When you declare a disaster, your vendor starts the provisioning process. Whether the workplace recovery center is fixed or mobile, this means setting up the required network connections within the vendor’s network so that the recovery center can connect with your data center. If you’ve signed up for mobile recovery services, one or more mobile recovery centers will be dispatched to your specified location. When they arrive, the trailers, generators, and satellite dishes will be deployed. After the

mobile center is up and running, the IT experts begin the long process of setting up all of the endpoints.

Whether mobile or fixed, this process is the same. Each PC needs its internal hard drive erased to ensure that your company cannot gain access to any of the information that might have been on it from a previous deployment. If you want the drives erased to US Department of Defense standards, the number of wipes may increase to 10, 20, or even 30. If the drives are large, this can take days. After the drives are erased and formatted, your gold master CDs are used to lay down the operating system configuration required to fit your environment. If the GM is old, the computers may need to be booted and then patched to the latest software, which can take more hours to days, depending on how many computers need to be provisioned and how out of date the GM CD is.

Secure Pocket Drive For Organizations

Secure Pocket Drive from SPYRUS is a bootable “PC-on-a-stick” device in which Windows Embedded Standard is bound to a bootable encrypting USB flash drive. Simply plug it into any computer and boot into a Windows XP- or Windows 7-compatible version of Windows Embedded Standard. While Secure Pocket Drive is read only to end users, system administrators can add it to a Windows domain and



push patches and settings to it by using Microsoft System Center Configuration Manager (SCCM).

Instead of imaging every computer in the recovery center, the IT staff plugs a Secure Pocket Drive into each computer and boots from it. Secure Pocket Drive can be stored at your company and brought to the recovery center when a disaster is declared or the vendor can keep them for you.

If the organization keeps them, either end users or the IT staff can boot and use Secure Pocket Drives on a periodic basis. Since Secure Pocket Drive is perfect for road warriors and teleworkers, why not assign them to individual employees and let them know that they are responsible for returning their Secure Pocket Drive to the IT department or bringing them to the recovery center when a disaster is declared.

Secure Pocket Drive For BC Vendors

If you are a business continuity vendor, think about how quickly you can bring up a customer's environment with Secure Pocket Drive. In fact, you could have one company in the center on Monday and another on Tuesday without needing to erase and re-image hard drives. No more worries about cross-contamination between customers if you forget to completely wipe a hard drive. Just keep

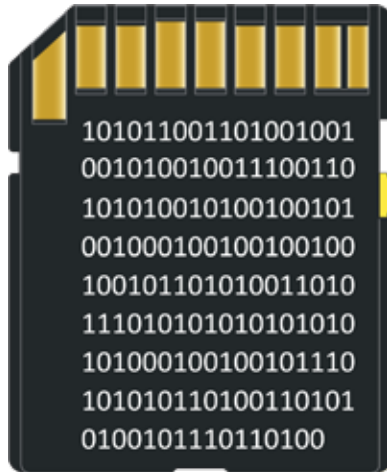
a stock of Secure Pocket Drives for each client and leave the hard drives out of the recovery center computers. When a disaster is declared, pull out the client's stock of Secure Pocket Drives, pop one into each computer, and boot. What could be faster and easier than that?

Summary

Secure Pocket Drive can be carried all the time as a laptop companion, so that your employees are not required to bring home their laptop and power supply every night in case they cannot come to the office the next day. When disaster strikes, Secure Pocket Drive can be used from home to create a secure environment owned and managed by your organization. If workers need to move to a temporary workspace or recovery center, then Secure Pocket Drive can be used to boot whatever PC happens to be available.

Without your workers, all you have is a data center, and that simply is not enough to keep your business running. But with Secure Pocket Drive in their pocket, employees can be productive anywhere that there is a PC with a network connection. And keeping your business running is all about keeping your employees working.





When powered off, Secure Pocket Drive is protected by XTS-AES 256-bit encryption.

ADDITIONAL INFORMATION

- Designed, engineered, and manufactured in USA
- FIPS 140-2 Level 3 compliant
- Secure pre-boot authentication
- No residue left on host PC—you were never there.
- Malware protection
- Sophisticated self-destruct mechanisms
- Works with government-issued CAC cards
- Computer BIOS must support booting from a USB drive
- Minimum 1GB RAM required, more is better

CERTIFICATIONS

- FIPS 140-2 Level 3 certificate 1394 for the sector-based encryption module
- FIPS 140-2 Level 3 certificate 1302 for the SPYCOS® hardware security module
- Common Criteria EAL 5+ certificate BSI-DSZ-CC-0315-2005 for the Infineon SLE66CX642P cryptographic processor

Proudly designed, engineered,



and manufactured in the USA



Microsoft Partner
Gold OEM Hardware

For more information about SPYRUS products, visit www.spyrus.com or contact us by email or phone.

Corporate Headquarters

1860 Hartog Drive
San Jose, CA 95131-2203
+1 (408) 392-9131 phone
+1 (408) 392-0319 fax
info@spyrus.com

East Coast Office

+1 (732) 329-6006 phone
+1 (732) 329-6211 fax

Australia Office

Level 7, 333 Adelaide Street
Brisbane QLD 4000, Australia
+61 7 3220-1133 phc
+61 7 3220-2233 fax
www.spyrus.com.au
info@spyrus.com.au



© 2011 SPYRUS, Inc. All rights reserved. Secure Pocket Drive is protected by U.S. Patents 7,757,100, 7,380,140, 6,088,802, and 6,981,149, with other patents pending. Individual Hydra PC products may embody technology protected by one or more of the following patents or patent applications: U.S. Pat. Nos. 6,088,802; 6,003,135; 7,757,100; 7,380,140; 6,981,149; 5,761,305; 5,889,865; 5,896,455, 5,933,504; 5,999,626; 6,122,736; 6,141,420; 6,336,188; 6,487,661; 6,563,928; 6,618,483; U.S. Pat. Appl. Ser. Nos. 12/018,094; 61/300,772; 09/434,247; 09/558,256; 09/942,492; 10/185,735; Can. Pat. Appl. Ser. Nos. 2176972; 2176866; 2202566; 2174261; 2155038; 2174260; E.P. Pat. Appl. Ser. No. 96201322.3; 97106114.8; 96105920.1; 95926348.4; 96105921.9; PCT/US08/51729; Israeli Pat. App. No. 199983; India Pat. Appl. No. 1422/MUMNP/2009. SPYRUS, the SPYRUS logo, Secured by SPYRUS, Hydra Privacy Card, Hydra PC, PocketVault, Digital Attaché, Rosetta, Rosetta Micro, Secure Pocket Drive, SPYCOS, and Security to the Edge are either registered trademarks or trademarks of SPYRUS, Inc., in the U.S. and/or other jurisdictions. All other company, organization, and product names are trademarks of their respective organizations.