FIBERLINK

PLANNING FOR A PANDEMIC:
TURNING OFFICE WORKERS INTO MOBILE WORKERS FOR BUSINESS CONTINUITY

A Fiberlink Communications White Paper

Table of Contents

Introduction

Enterprises are being forced to take a new look at their business continuity and disaster recovery plans because of the prospect of pandemics – epidemics affecting wide geographical areas for weeks or months.

Planners are contemplating new scenarios in which contagious diseases like SARS and avian influenza limit travel and prevent workers from congregating in offices.

The striking new challenge is how to maintain employee productivity when the workforce is confined to their homes or other remote locations. As one executive put it, "How can a company go from 20% of its employees working outside of the office to 70%?"

This white paper looks at some of the key issues facing enterprises that might need to turn office workers into mobile workers, rapidly and in large numbers. It examines:

- The technical and human challenges of supporting business processes during a pandemic.
- The planning required.
- Procedures to equip employees with the information and technology to remain productive.
- Potential impact on the infrastructure and on support staffs.

The final section of the white paper describes how services from Fiberlink can help quickly and cost-effectively provide security and connectivity for remote employees during a pandemic, or as a response to other types of disasters.

What is Different about Planning for a Pandemic?

A DIFFERENT TYPE OF DISASTER

The outbreak of SARS in Asia in 2003 and the threat of a human-communicable version of avian influenza have forced enterprises to consider a new type of disaster – epidemics affecting wide geographical areas for extended periods.

Tragically, the danger of pandemics was graphically illustrated in the early 20th century, when the Spanish influenza outbreak infected about 20% of the worldwide population and resulted in over 50 million deaths. The Asian flu pandemic of 1957 killed 69,000 in the United States alone, despite the availability of vaccines. Yet, looking ahead, there is not yet a commercially available vaccine to protect humans against avian flu. The World Health Organization projects potential fatalities from an avian flu pandemic to exceed two million worldwide, even in their "conservative" planning scenario.

Should such an outbreak occur in the near future, government bodies and health organizations will impose quarantines, restrictions on travel, and drastic limitations on people congregating in public places.

So, while most business continuity and disaster recovery planning before 2003 focused on protecting data and providing extra capacity to cope with a sudden loss of infrastructure, planners must now prepare for scenarios where infrastructure remains intact, but workers are unable to congregate in offices, or even leave their homes, for weeks or months at a time.

> Some companies have discovered that while they back up their servers or data centers, they've overlooked backup plans for laptops. Many businesses fail to realize the importance of data stored locally on laptops. Because of their mobile nature, laptops can easily be lost or damaged. It doesn't take a catastrophic event to disrupt business if employees are carting critical or irreplaceable data around on laptops.
>
> –The ABCs of Business Continuity and Disaster Recovery Planning, CSO Online
> (http://www.csoonline.com/fundamentals/abc_continuity_2.html)

NEW ISSUES FOR BUSINESS CONTINUITY PLANNING

Most aspects of business continuity and disaster recovery planning apply to pandemics just as much as to fires, hurricanes, floods, earthquakes, terrorist attacks and other natural and man-made disasters. However, there are a few topics that require special emphasis.

Emergency Communication

While emergency communication is important in any disaster recovery scenario, it is particularly critical in the event of a pandemic. Since employees and their families may be personally threatened, and since they may be exposed to rumors and panics, it is particularly important that they receive accurate, up-to-date information on health issues. Employees also need detailed information on company policies and procedures for working in the new environment, and open communication channels to company officials to help resolve personal and work-related issues in high-stress situations.

Endpoint Security and Connectivity

Enterprises must plan to provide secure, reliable connectivity and access to corporate networks for employees who are suddenly forced to work in their homes, hotels, or other remote locations.

Administrators must plan for distributing software to remote computers, for ensuring security on computers outside of the corporate firewall, and for providing backup and data encryption capabilities to mitigate the risk of mobile devices with sensitive data being lost or stolen.

Collaboration and Re-Engineered Processes

Planners must prepare for ways to re-engineer business processes so they can continue without face-to-face interaction between employees. This might include providing employees with collaboration tools, modifying business applications to automate processes that had been handled by informal and "sneaker-net" methods, and introducing workflow and project management tools that help managers control processes across multiple locations.

Enterprises must also anticipate a dramatic increase in requests for technical support and questions for Human Resources and other groups who provide information and support for employees working under unfamiliar conditions.

This paper will discuss procedures to address these challenges in three areas:

- Planning, testing, and preparation.

- Supporting employees and remote computers.

- Preparing IT, support, and the office infrastructure.
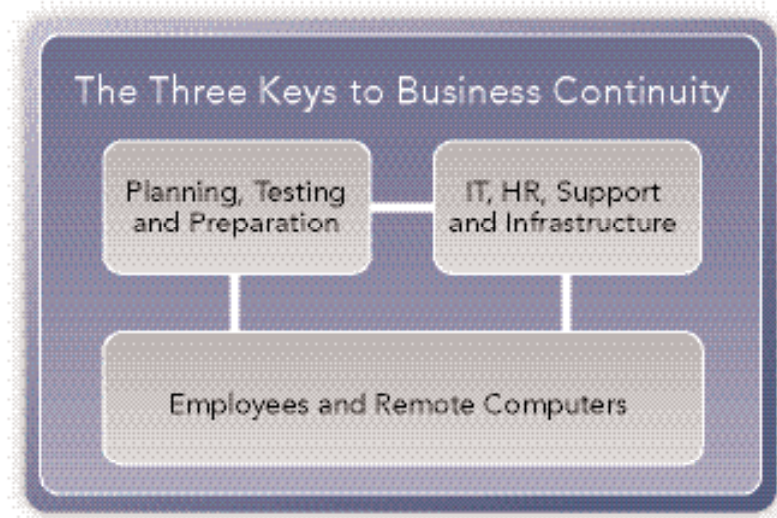
1. Planning, Testing and Preparation

While standard methodologies for business continuity and disaster recovery planning can be applied to all types of emergencies, experts suggest a number of variations related to the specific challenges created by pandemics.

Explore a variety of scenarios

Enterprises should explore a variety of pandemic scenarios. These might start with a low-level threat affecting a circumscribed geographic region, and range up to a widespread pandemic with severe government-imposed restrictions on travel. The number of employees affected, the reactions of medical and governmental organizations, and the behavior of customers and suppliers should be examined across these scenarios.

Identify key processes and individuals

Not every business process can be re-established immediately after a crisis. Therefore it is important to identify which processes are critical and must continue with minimum interruption and maximum efficiency, and which processes that can afford some interruption and temporary inefficiencies. This analysis will also help identify which individuals should be given first priority for reconnection and support.

Examine endpoint security, connectivity and productivity

In the event of a pandemic, enterprises will need to turn office workers into remote and mobile workers rapidly and in large numbers. This poses major challenges in the area of endpoint security, connectivity, productivity and end user support. The planning team will need to understand thoroughly how these challenges apply to their environment, then develop policies and technical solutions to address them. These topics are discussed in the next section of this white paper.

Create manuals for everyone

Because a pandemic can affect every part of an organization for an extended period, it is advisable to document emergency policies and procedures for many affected groups. This might include a:

- "Mobile Operations User Guide" for employees.
- Manual or extended knowledge base for the technical support staff.
- Special policy handbook for Human Resources personnel.

Prepare additional communications channels

It is critical that employees and their families receive accurate, up-to-date information on health and work issues immediately in the event of an emergency. Planners may want to put in place mechanisms for email and voicemail blasts, or even for automated telephone contacts using an Interactive Voice Response (IVR) system. These systems may need to be integrated with corporate directories or Human Resources databases to make sure employee contact information is always current.

Employees will also need to obtain plans and procedures over an extended period of time, so planners should prepare to use collaborative tools or a section of the corporate intranet as a repository for emergency documents.

Run exercises with typical employees

Many types of disaster recovery plans can be tested with the participation of technical staffs only. However, tests of plans for pandemics must be carried out with typical employees in real-life conditions. This is because conditions in users' homes are varied and unpredictable, and because employees and managers may need to experiment and develop new methods for maintaining business processes while working remotely.

Some organizations have addressed this challenge by asking a large group of employees to stay home and work remotely for a period of time (a day to a week). The loss of short-term productivity is considered an investment in creating a business continuity plan that will stand up to unnerving real-life conditions.

Prepare critical employees in advance for remote access

A number of organizations have taken the view that they should fully prepare critical employees for remote operations well in advance of an actual crisis. "Critical employees" include top executives, staff members involved in responding to the emergency, and managers and workers who support the most critical business processes. These employees can be provided with laptops that contain all the software needed for remote operations (or alternately, PCs already in their homes can be brought up to corporate standards). These employees can also be given adequate Internet connectivity (typically broadband) from their home or alternate workplace, and all of the documentation and communication links needed to begin working remotely without delay.

Line up software, hardware and services for emergency deployment

Obviously, it is not economical to fully prepare all employees in advance for remote access, but organizations need to line up resources in advance to enable office workers to become mobile workers shortly after a crisis breaks out. They can acquire software licenses for remote systems, stockpile extra hardware and software to handle more Internet traffic into the corporate networks, and make prior arrangements to obtain contract services from outside parties. Some vendors offer special arrangements to provide "contingency" software licenses or services at a low cost on a contingency basis, where the full cost is charged only if and when the licenses or services are used.

2. Supporting Mobile Employees and Computers

The challenge of preparing employees to work from their homes and other remote locations comes to the forefront in planning for pandemics. Compared with other forms of disaster recovery planning, planners must put a much greater emphasis on communications and collaboration, and also on technologies that can help improve the security and connectivity of mobile computers.

Set up two-way communications

In the event of a pandemic, employees need accurate information to counteract rumors and to inform them of company policies and procedures. They also need to be able to find a "Mobile Operations User Guide" and other documentation that provides information on how to work from home. Useful communication media include email and voicemail blasts, Interactive Voice Response systems, and the corporate Intranet.

Communication needs to flow in both directions. Employees will want to ask questions to technical support and Human Resources staff. Employees and managers can become productive more quickly if they can consult experts and exchange information among themselves about new ways of doing business in this extraordinary environment. To meet these needs planners can post directories of key support personnel and set up bulletin boards, chat areas and knowledge bases to allow employees to share ideas on coping with work and personal issues.

Prepare software distribution and Web-based applications

Distributing, installing and updating software on remote computers is extremely challenging when dealing with employee-controlled laptops, and even worse, employee-owned home computers. Obstacles include unpredictable combinations of applications and release versions, requirements for drivers and software patches, software installations that overwrite each other, and huge files that need to be downloaded over slow connections.

Enterprises can prepare for these software distribution challenges by investing in software distribution tools and by writing installation scripts. Another approach is to switch to browser-based applications (including Web email clients) and to use thin-client terminal server architectures where appropriate.

Some enterprises choose to keep a stock of laptops that can be given to critical employees at the outbreak of a crisis, preloaded with all required software.

Ensure endpoint security

Security is another critical and challenging area for mobile computing. Home workers, "road warriors" and other mobile employees are exposed to hackers, viruses, spyware, Trojans and many other threats, yet lack the protection of the corporate firewall and other defenses.

In fact, organizations may be particularly vulnerable to security threats during pandemics. First, hackers and virus writers may be emboldened by chaotic conditions to increase their attacks. Second, overwhelmed support and security staff may have less time than normal to monitor, detect and respond to threats.

Administrators must ensure that:

- A full range of security applications is installed on all remote systems, including a personal firewall, anti-virus and anti-spyware tools.

- Virus signature and other threat databases are kept updated.

- The operating system and other key software components have been updated with the latest security patches.

- Software for a VPN client and for strong authentication (if appropriate) is available on the systems.

- All of the above are in place and actually operating before remote systems are allowed access to the corporate network.

- There is visibility into whether remote systems are in fact in compliance with enterprise policies and best practices.

While it is normally quite difficult to guarantee that these conditions are met on a mobile computer, this capability can be provided by the Fiberlink solution, which is discussed in the last section of this white paper.

Protect against data loss and theft

In a pandemic scenario, it is inevitable that large amounts of sensitive and critical corporate data will be generated or stored on computers outside of the office. Unfortunately, laptops are extremely vulnerable to loss and theft, as demonstrated by a few highly publicized recent incidents. These risks may be heightened during a pandemic because of chaotic conditions and the disruption of normal police activities.

For these reasons mobile computers should be provided with:

- Backup mechanisms, so critical data can be recovered if the computer is lost.

- Data encryption, so sensitive data cannot be read if the computer is stolen.

Provide simple, flexible connectivity

Providing simple connectivity to the Internet can be a major challenge when a large number of office workers are converted to mobile workers. Without proper tools and support, employees trying to connect for the first time can become baffled and frustrated. Even experienced mobile users can encounter problems trying to connect from unfamiliar locations.

Connectivity also needs to be flexible. Employees with a broadband connection at home may need to use a dial-up connection from a friend or relative's house. Employees stranded in remote locations may want to take advantage of broadband services in hotels, or Wi-Fi hotspots in airports, cafes, and other public venues.

Fortunately, there are a variety of connectivity services that can simplify connectivity for employees. This can dramatically reduce the number of support calls, as well as boost employee productivity. One such service from Fiberlink is described later in this document.

Set up an infrastructure for SSL VPNs

Many organizations are exploring the use of SSL VPN (Virtual Private Network) technology to provide secure connectivity with mobile employees. SSL VPNs take advantage of the Secure Socket Layer encryption that is built into Web browsers to encode information traveling between remote systems and the corporate network. This eliminates the need to deploy a separate VPN client to the remote systems. It also can be used to create a temporary secure connection to computers that do not belong to the enterprise or its employees, such as PCs belonging to customers or to Internet cafes.

Organizations that want to use this technology need to acquire software, hardware and experience so that they can expand the use of SSL VPNs rapidly in the event of a crisis

Enhance collaboration and streamline business processes

A pandemic would abruptly deprive employees of accustomed face-to-face contact and paper-based workflows. To prevent a drastic fall-off in productivity, employees need to be provided with collaboration tools such as audio and video conferencing, bulletin boards and discussion forums, searchable knowledge bases, shareable document repositories and file systems, and corporate-sanctioned instant messaging.

To track and control projects and complex tasks, physical supervision by managers can be replaced with computerized workflow and project management tools, and by content management systems.

Business continuity planning can provide a valid rationale for re-examining and re-engineering business processes. Simplifying and automating these processes can make them easier to support when users are at remote locations.

Be prepared to deal with home PCs

Employees with no laptop or portable desktop PC may be forced to work from an employee-owned home PC. This can be particularly painful for the IT group, because home PCs are far more likely than corporate devices to be old, infected, and cluttered with software that interferes with key business applications. Also, these PCs may be shared by several family members.

For critical employees, the IT department may want to keep a stock of preloaded laptops that can be distributed at the outbreak of a crisis.

However, for those employees where there is no option except home PCs, enterprises can put in place technologies that are able to inventory home PCs to ensure that they meet enterprise standards, and can download and install key security and connectivity software.

3. Preparing Support and Office Infrastructures

Standard methodologies for business continuity and disaster recovery cover most of the issues related to preparing the IT department and the office infrastructure. These include data backup and recovery, distributed data centers with redundant capacity, and preparedness plans for the technical staff. However, there are a few areas that require additional emphasis when preparing for a pandemic.

Prepare for a surge in remote connections

As office workers turn into mobile workers, the volume of remote connections will increase sharply, so enterprises need to have adequate hardware and software licenses to handle this surge. In addition to routers and networking equipment, this may include VPN concentrators, software and hardware for SSL VPNs, servers to manage user authentication, and servers or appliances for perimeter security applications such as firewalls and intrusion protection.

The support group must ensure that it has the methods to set up new mobile users quickly and give them access rights to the proper resources within the enterprise network.

It is also important that alternative points of ingress to the corporate network are established, in case one or more are disabled. This could happen if technical staff members are unable to remain at a data center or NOC.

Equip support staffs to assist first-time mobile users

In the event of a pandemic, technical support and IT staffs will be called upon to assist employees whose only experience has been using computers on a corporate LAN. Support organizations may require special training in how to work with confused and technically inexperienced end users.

Support staffs should also be given tools that make remote support easier, including tools to inventory software and hardware on remote systems, "remote control" software to help diagnose and solve problems, and software distribution tools.

How Fiberlink Can Help Turn Office Workers into Mobile Workers During a Pandemic

Fiberlink: Technology to support mobile and remote employees

An unprepared IT organization, in the event of a pandemic, would be forced to integrate, deploy and manage a wide range of new technologies, for a dramatically enlarged pool of inexperienced mobile and remote employees, under extremely challenging conditions. The chances of success, or even survival as a functioning enterprise, would be small.

Fortunately, in addition to planning and preparing, organizations can take advantage of the work of companies who have already done the work to integrate technologies and tools for mobile work.

Since its inception in 1994, Fiberlink has been a leader in delivering products and services to make mobile and remote computing secure, simple and cost-effective.

Over 700 enterprises around the world have worked with Fiberlink to improve security, reduce networking and support costs, and simplify the connectivity experience of mobile employees.
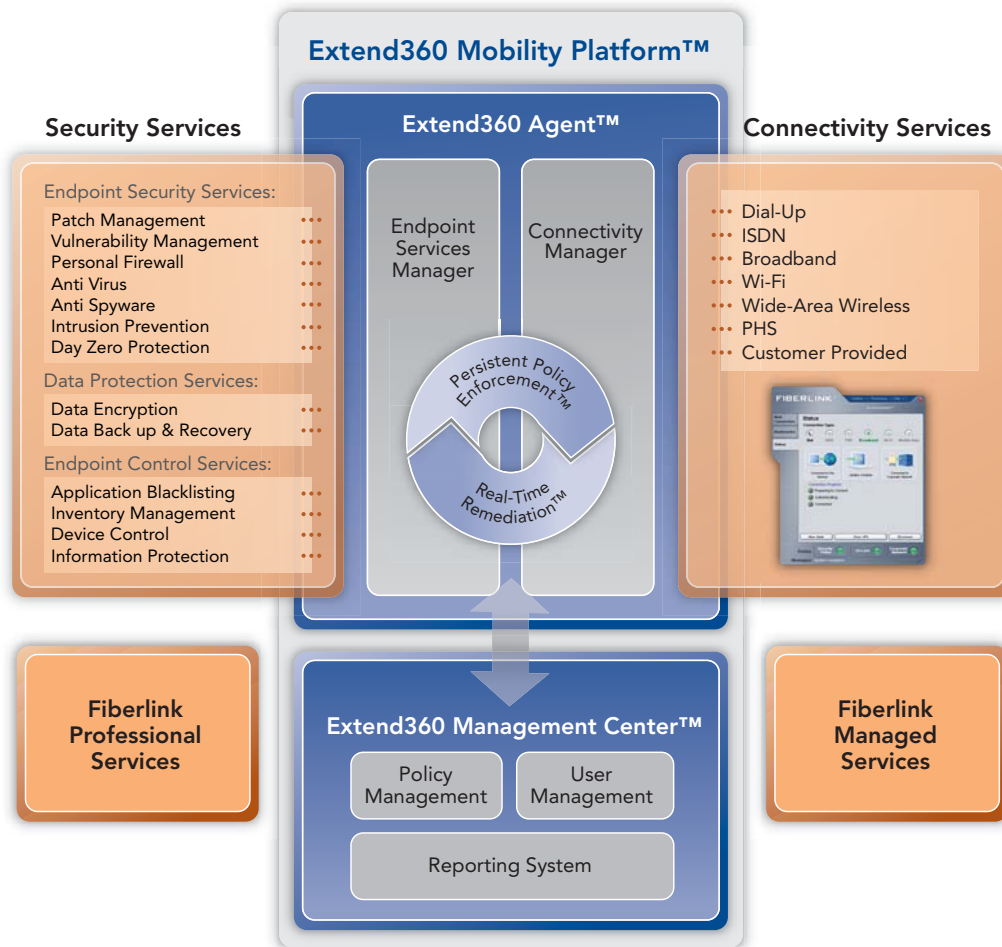
Figure 1: The Extend360 Mobility Platform™ and Fiberlink Security and Connectivity Services

Fiberlink offers:

- The Extend360 Mobility Platform™, a software platform for managing security and connectivity applications on mobile and remote devices.

- Fiberlink Security Services, a set of services to deploy and manage endpoint security, data protection, and endpoint control applications on mobile devices.

- Fiberlink Connectivity Services, an aggregated virtual network that provides Internet connectivity through 65,000 access points around the world using dial-up, broadband, Wi-Fi and other connection types.

Fiberlink's software platform and services allow enterprises to:

- Deploy, monitor, update and remediate a wide variety of endpoint security applications on remote computers, including personal firewall, intrusion protection, anti-virus, anti-spyware, patch management, backup and recovery, data encryption, and VPN client software.

- Provide employees with one-click connectivity to all major network types – dial-up, ISDN, DSL and cable modem broadband, Wi-Fi, and wide area wireless protocols such as CDMA, EV-DO and GPRS.

The components of the Extend360 Mobility Platform™, Fiberlink Security Services, and Fiberlink Connectivity Services are illustrated in Figure 1.

Fiberlink also offers:

- Professional Services to help customers deploy and manage an effective mobile computing infrastructure.

- Managed Services to outsource the administration of software and devices for authentication and perimeter security.

The early sections of this white paper discussed the challenges of turning office workers into mobile workers in the event of a pandemic; this final section describes how Fiberlink can help address many of these difficult challenges.

Ensuring endpoint security

Mobile laptops and home computers are exposed to hackers, viruses, spyware, Trojans and other threats without the protection of the corporate firewall and other perimeter defenses. A hacker who gains control of a remote PC could not only steal data stored on that PC, but could potentially use its VPN connection to tunnel directly into the corporate network. This could expose the enterprise to data theft, sabotage, non-compliance with government regulations, and other very serious security breaches.

The Extend360 Mobility Platform allows enterprises to deploy and manage a wide variety of endpoint security applications on mobile computers. These applications include:

- Personal firewalls and intrusion prevention systems (IPS), to block hackers.

- Anti-virus and anti-spyware tools, to block viruses and spyware programs.

- Patch management and vulnerability management tools, to keep operating systems and other key software updated with security patches.

- Zero-day protection, to quarantine new varieties of malware before they can be identified by standard anti-virus and intrusion protection systems.

- VPN software, to create secure connections from remote systems to corporate networks.

Fiberlink's software can install these applications on demand, as well as ensure that configuration files, virus signatures and other threat signatures are kept updated. It can also provide remediation services, so if any of the applications are found to be inoperable, they can be repaired (for example by downloading files and rewriting registry entries) and restarted.

Finally, the Extend360 Mobility Platform™ can protect corporate resources through Mobile-NAC (Network Access Control): the ability to block remote computers from connecting with enterprise networks unless they are in compliance with corporate security standards.

Fiberlink's services work with a wide selection of best-of-breed personal firewall, anti-virus and anti-spyware packages, so in most cases, enterprises can preserve their investment in existing endpoint security software.

Taken together, Fiberlink's technology services drastically simplify the task of deploying and supporting a complete set of security applications on mobile laptops and desktop computers.

Protecting against data loss and theft

A great deal of key business information and sensitive data are already stored on laptops today, and the amount is likely to increase sharply in the event of a pandemic.

Fiberlink offers a backup and recovery service that allows data to be stored off-site and recovered if a computer is lost or damaged.

Fiberlink's Extend360 Mobility Platform can manage a data encryption application that prevents sensitive information from being read if a computer is lost or stolen.

Fiberlink also offers services that can prevent the copying and distribution of sensitive information by unethical or reckless employees. Fiberlink Device Control service can block users from copying information to removable devices such as USB memory sticks and CD-ROM drives. Fiberlink Information Protection service controls "information in motion" by preventing employees from distributing confidential information by email, saving it to portable devices, transmitting it with instant messaging or file transfer programs, or even printing it.

Given the disruption and confusion inherent in any disaster scenario, these services from Fiberlink can prevent or mitigate the severe risks associated with the loss or theft of key data.

Providing simple, flexible connectivity

Providing connectivity to the Internet can be a major challenge when a large number of office workers are converted to mobile workers.

Fiberlink's Extend360 Mobility Platform makes connectivity as simple as possible for mobile and remote workers. The software detects all of the connection options that are available and allowed for that user – dial-up, ISDN, PHS, broadband, Wi-Fi and mobile data (cellular wireless) – and lets the user select from among them with one click. The software handles the connection, including launching an SSL or IPsec VPN connection if required.

If employees are sent to new locations, Fiberlink's client can be sent a variety of VPN profiles and dial-up telephone numbers for those locations to take advantage of low-cost local access points.

This ease of use and simplicity allow mobile employees to connect to enterprise networks without extensive training, and without becoming frustrated. It also dramatically reduces the cost of supporting these users.

Providing comprehensive, global connectivity services

Fiberlink's Connectivity Services add a critical layer of redundancy and additional capacity to an enterprise's connectivity options. Mobile employees can take advantage of Fiberlink's agreements with Tier 1 ISPs, DSL and cable service providers, hotel broadband service providers, Wi-Fi hotspot service providers, and cellular and other wireless carriers. In all, Fiberlink's customers can utilize 65,000 access points in more than 150 countries.

This virtual network gives enterprises true global coverage, which is ideal in case employees are forced to work in countries where an enterprise has no contracts with local service providers. It gives employees the opportunity to use any appropriate network type (dial-up, broadband and wireless) in any location. And it provides redundancy and an increased chance of getting through if an individual local service provider is overloaded.

Supporting emergency communications

Fiberlink's Extend360 Mobility Platform™ can assist with emergency communications by automatically downloading documents to users' computers and placing them on the desktop or in a specified directory. For example, at the time of a crisis the Extend360 Mobility Platform could place a set of emergency instructions, a list of email addresses and links to key documents on the corporate Intranet, and a "Mobile Operations User Guide", right on an end user's desktop.

Distributing key software applications

Fiberlink's software can download and install a core set of applications and browser plug-ins. These include security applications, VPN clients, and some productivity and business applications. In an emergency, this can allow mobile workers to establish secure connections and begin working without support from the IT department.

Managing an SSL VPN infrastructure

Fiberlink offers a managed service to administer SSL VPN software and hardware. Instead of setting up their own infrastructure to manage SSL VPNs, enterprises can outsource this activity to Fiberlink.

Dealing with home PCs

Fiberlink's technology can provide invaluable help in turning uncontrolled home PCs into secure business computers.

The Extend360 Mobility Platform can collect and report on inventory information from PCs to determine if they meet minimum hardware, software and release level standards. This step can be taken either at the time of need, or as a preparatory step well in advance of the crisis.

When an emergency occurs, Fiberlink's software can install and manage endpoint security applications in order to detect and remove viruses, spyware, Trojans, zombies and other security threats.

The Extend360 Mobility Platform can also block the execution of specified software applications. This prevents games, file sharing programs and personal applications from interfering with the operation of business applications, and can stop the use of instant messaging and other applications that create security risks.

FIBERLINK'S MOBILE PREPAREDNESS PROGRAM FOR BUSINESS CONTINUITY

Fiberlink offers a special Mobile Preparedness Program designed to help organizations put in place technology and precesses that can turn office workers into mobile workers in the event of a pandemic, natural disaster, or other emergency situation.

Elements of this program include:

- A Business Continuity Emergency Condition License (BC-ECL_ which allows Fiberlink's Extend360 Agent ™ to be installed on laptops and remote PCs and used for up to eight weeks during emergencies. The cost of this license is a fraction of Fiberlink's standard licesne rate.

- A policy and spftware update that allows the organization's custom Extend360 Agent™ configuration to be updated four times annually. This allows organizations to change security and connectivity policies as their environments change.

- A Profession Servies assessment of the organization's requirements for mobile security and connectivity in the event of a pandemic or other threat to business continuity.

- Optional arrangements to host the infrastructure for SSL VPNs, RADIUS servers, and two-factor authentication. These facilities can help enterprises handle a surge in remote access requests without having to purchase additional VPN concentrators or RADIUS servers..

START GETTING RESULTS TODAY

Fiberlink's offerings can produce an immediate return on investment at the same time as they prepare enterprises to cope with the effects of disasters in the future.

Fiberlink's technology can increase the security and simplify the experience of mobile workers right away, even as it prepares them to cope with extraordinary conditions in the event of a disaster. It can reduce networking and support costs immediately, as well as addressing the networking and support issues of the future.

Enterprises that have a significant number of mobile and remote employees – "road warriors," telecommuters and "day extenders" (people who take their laptops home at night and on weekends) – can talk to Fiberlink about improving endpoint security and connectivity today, as well as planning for the unknowns of tomorrow.

FOR MORE INFORMATION

For more information on Fiberlink's technology and services, contact Fiberlink at:
1787 Sentry Parkway West, Building 18, Suite 200; Blue Bell, PA 19422
Phone 215.664.1600; Fax 215.664.1601
www.fiberlink.com