

# Preparing for a Pandemic

Guidelines to help your agency support direct responses and continue operations during a disaster situation

## TABLE OF CONTENTS

- 2** Priorities for Pandemic Preparation
- 3** Secure Networking
- 4** Server Management
- 4** Remote Access and Communications
- 5** Unified Communications
- 6** Asset Management
- 7** Data Storage and Power Management
- 8** Manufacturer Options

## Executive Summary

The spread of the H1N1 flu brings into sharp focus the need for government agencies to prepare for a pandemic's potential impact on their operations and on their communities at large.

While disaster planning and the creation of a continuity of operations plan have been priorities in most organizations for some time, a pandemic is a crisis with unique features. Its beginning and (most importantly) its end are cloaked in uncertainty.

Although the impact of any disaster lasts much longer than the event itself, the actual duration of a pandemic can extend for months or years, with new waves of infection building unexpectedly. And, of course, a pandemic is by definition a global emergency.

While preparing for a pandemic, planners must be mindful of their agency's role in the frontline response to the health emergency, as well as the need to fulfill the agency's mission despite restrictions that might be imposed. All these factors suggest that upgrading and extending the organization's communications and information management infrastructures should be central considerations in any pandemic preparation strategy.

This white paper explains how key technologies can help prepare organizations to both support direct responses to the pandemic and continue their own operations. Fortunately, the steps outlined will also pay dividends in more efficient and effective daily operations, as well improved response to localized emergencies.

.....

## Priorities for Pandemic Preparation

For planning purposes, the response to a pandemic can be broken into several clear priorities. Each aspect of the response will place strains on the technology infrastructure that need to be addressed in any preparation strategy.

### Social Distancing

This strategic step comprises plans aimed at separating people in order to prevent the spread of an infectious disease. School closings, cancellation of large public gatherings and restrictions on mass transit systems are social distancing measures likely to be taken early in response to a pandemic emergency. Those steps may be followed by the closure of office buildings, or restricting access to “essential” personnel in a government or public safety agency.

But few organizations can perform vital functions with substantially reduced staffs, so a technology infrastructure must be in place that supports efficient teleworking.

The challenges social distancing poses to IT involve upgrading and extending networks, as well as deploying systems that will provide staffers working in their homes with secure remote access to applications and data they need. Planning and implementing such projects can take months, so they need to be in place before a pandemic spreads.

### Supporting Mass Prophylaxis and Triage

In the event of a pandemic, mass prophylaxis and triage sites will be designated to intervene in the spread of infectious disease, as well as to diagnose and treat the illness. Thousands of new patients in need of inoculation, quick evaluation and/or care may overburden the existing healthcare infrastructure and require the establishment of ad hoc prophylaxis and triage sites in public places, such as convention centers and sports arenas.

IT preparation for this aspect of pandemic response involves developing a robust mobile communications infrastructure. In addition, the IT department must be ready to provide the hardware, software and communications links necessary to support provisional mass prophylaxis sites with remote access to applications and information. Both physical and network security must be priorities in these highly vulnerable operations.

### Resource Accountability

Federal regulations require that all resources used in response to a pandemic emergency (personnel, assets and inventory) be tracked and managed electronically. Beyond legal and economic implications, maintaining real-time accountability of assets is crucial to deploying them effectively to slow the spread of a pandemic and mitigate its impact.

Accountability will be more difficult to sustain as organizations try to function with staffs depleted either by illness or social distancing measures. A changing environment of quickly deployed prophylaxis and triage centers can put a strain on accountability too.

The challenge for IT is to develop systems for electronic accountability that can be used by responders with little or no technical training. Those systems must also be capable of being deployed remotely and operating over a limited or diminished communications infrastructure.

### Force Multiplication

A spreading pandemic will not spare first responders or the staffs of other government agencies. Therefore, technologies that act as force multipliers — those facilitating the use of auxiliary personnel and increasing the efficiency and productivity of the functioning workforce — will be crucial.

The need for force multiplication will be heightened by the pressures of creating and maintaining mass prophylaxis centers and tracking all the resources mobilized to combat the pandemic.

If workers from nongovernmental organizations, other levels of government and trusted private partners are pressed into service, technologies such as reliable, easy-to-use credentialing systems will be important. Force multiplication measures offer increased efficiency and productivity during normal operation and can become a lifeline for response activities to a public health emergency.

### Inter- and Extra-governmental Coordination

The rapid and unimpeded flow of information will be essential when coordinating the response to a pandemic by various agencies and levels of government, as well as by private institutions and the public. Building and maintaining secure, interoperable and resilient communications systems is a must.

In a widespread public health emergency, interoperability among communications systems and technologies has to be a prime consideration. In addition, technologies have to be in place to support mass notification of critical information and emergency instructions to the public. Taking steps to maximize the reach, flexibility and resilience of communications systems is the best preparation for a coordinated response to a pandemic.

## Secure Networking

Creating a secure networking infrastructure is part of the preparation for all aspects of the response to a pandemic. Networks will need to handle dramatically increased loads, which will include highly sensitive health and public safety information.

Without secure networks in place, social distancing measures will limit or halt the operation of most government offices. Coordination among government agencies will also break down, with a resulting impact on the operation of mass prophylaxis sites and efforts to track and manage resources.

Implementation of technologies such as virtual private networks (VPNs) will support coordination of large-scale operations as well as cooperation among geographically separated coworkers. Encryption and authentication technologies can be used with VPNs, but are also applicable at any point at which officials want to protect data and control access to systems.

The ability to manage remote networks and also perform the management remotely will be crucial under the fast-changing conditions of a health emergency in which data centers may be inaccessible or understaffed.

### IPsec: Hardening the VPN Tunnel

IP security (IPsec) protocol provides beefed up security for data moving over the Internet through enhanced encryption and authentication. The protocol uses two modes of encryption — tunnel and transport:

- Tunnel mode, generally used in VPNs, encrypts both the header and the payload of any data packet;
- Transport mode just encrypts the payload.

**BROADBAND ROUTERS:** A broadband router, also known as a residential gateway, acts as a network switch with a firewall and facilitates the creation of home networks with connections to larger networks, usually the Internet.

The technology supports file sharing as well as various high-speed communications applications, such as e-mail and IP telephony.

Broadband routers can work with either wired or wireless Ethernet connectivity, and mobile options can be useful in the context of a pandemic response.

**VIRTUAL PRIVATE NETWORKS:** VPNs are private networks that operate over the Internet or other large public telecommunications networks via virtual connections. A VPN is a tunnel through the transport network that can be protected by layers of security technology.

When selecting a VPN product, agencies should consider factors such as scalability and ease of provisioning, and whether the vendor supports a full range of endpoint devices: PDAs, smartphones, desktop and notebook computers, and thin clients.

It’s also important that the VPN provides security that matches the needs of the organization — firewall features, modes of encryption (symmetric or public key) and access control options should all be explored. In a pandemic, easy access to remote help desk support will be important, especially to responders without technical expertise.

**ENCRYPTION AND AUTHENTICATION:** These are technologies designed to ensure that information is only accessible to users with appropriate credentials.

In the context of secure networking, encryption is the process of encoding data before transmission over a VPN or other network, and then decoding it at the receiving device. Authentication technologies verify the identities of authorized users via passwords, smartcards or biometric factors such as fingerprints, and then provide the appropriate level of access to the user.

Many organizations rely on AAA (authentication, authorization and accounting) servers for this function, with the “accounting” aspect providing a way to track usage. AAA servers can be used with, or replaced by, identity and access management software. In the context of emergency preparation, special care should be taken to ensure that stand-alone credentialing solutions or credentialing features of comprehensive access control systems are easy to use remotely.

**REMOTE NETWORK MANAGEMENT:** Preparation for a pandemic necessarily includes evaluating and possibly upgrading tools and strategies for managing remote networks. With increased numbers of remote sites and mobile workers, monitoring and management systems that provide a view into every tendril of the network, along with the ability to address any detected problems, becomes essential.

Conditions during a healthcare emergency will likely include rapid and somewhat ad hoc network expansion and require that IT teams take a hard look at the flexibility and scalability of their network management tools. During a pandemic, access to and staffing of the data center may be limited or uncertain, so IT staff should also be able to use any network management tools remotely.

## Server Management

While preparing for a pandemic emergency will draw attention to the edges of the IT infrastructure, organizations ignore the needs of the data center at their peril. None of the preparation steps outlined previously are likely to work without an optimized, well-maintained data center.

During a pandemic, managing and maintaining the data center will fall to a reduced IT staff, and team members may be asked to perform those tasks remotely. Streamlined server architecture and ease of management have to be priorities.

**SERVER CONSOLIDATION:** A server consolidation project should begin with a comprehensive blueprint of the organization's IT infrastructure including servers, PCs and other user devices, network elements, storage devices and key software. This step will provide a map of the technology terrain that will save time and effort in daily operations and become invaluable during a pandemic or other emergency.

Once the IT infrastructure has been mapped and evaluated, server consolidation within and among data centers takes several forms:

- Physical consolidation involves moving all the resources from multiple servers (print, file and storage) to fewer servers with greater capacity.
- Virtual consolidation moves computing resources from physical servers to software, or virtual, servers that run on a smaller number of physical servers.
- Consolidations of application or web servers are unique because they typically have higher request rates and reliability requirements than other servers.
- Data center consolidation is the process of bringing the servers from multiple data centers and/or remote sites together into a central data center. This usually involves server consolidation on either physical or virtual machines.

### PHYSICAL AND VIRTUAL SERVER MANAGEMENT:

Using hosted data center services can be an effective strategy for government agencies. Concerns about sensitive data and processes have slowed a wider embrace of hosted services by the public sector. But the advantages of the approach — savings in time and resources, availability of specialized expertise and high levels of redundancy to ensure operations continuity — make hosted services worth considering.

The majority of organizations that keep server management in-house will manage through one of the many software systems available. These provide integrated interfaces through which IT administrators can monitor servers and other resources in the data center and remote sites. Capacity planning, load balancing, provisioning and targeted maintenance and upgrading can be done from a central or (and this could be important during a pandemic) remote location.

For all of its benefits, a virtualized server environment can result in new complexities that must be addressed. Virtual servers add a layer of management, since the physical machines they run on need managing as well. Because provisioning new virtual machines is relatively easy compared to provisioning for physical servers, server sprawl can become at least as much of a problem.

Management systems for virtualized environments, such as VMware's vCenter, allow IT staff to view resources in the aggregate and allocate them dynamically based on the needs of the organization or situation. The promise of virtualization is tremendous, but IT departments should consider how well systems that manage virtual machines integrate with similar systems in place of the physical environment.

## Remote Access and Communications

The value of remote access and communications technology during a pandemic cannot be overstated; nor can the importance of maximizing communications systems in advance of a public health emergency.

Optimized communication technology will facilitate telework, connect mass prophylaxis and triage centers, act as a conduit for critical information about resources and provide the infrastructure for a coordinated response to the emergency. Finally, communication

technology is a powerful force multiplier, making it possible to use human and other resources as effectively as possible.

**CLIENT ACCESS:** Preparation for a pandemic begins at the endpoint of the communications infrastructure, which is the method or device through which users access information and applications. Under normal operating conditions, desktop and notebook computers are the most common user device, even for teleworkers.

Those devices will continue to be at the center of an emergency communications strategy, but increased consideration should be given to delivering information to netbooks, PDAs, smartphones and other portable devices. Key applications must run on a broad range of devices, especially during a pandemic.

## Virtual Reality

Although development, desktops and applications have gone virtual, there are three basic forms of virtualization:

- Server virtualization disconnects the physical characteristics of server hardware from the software running on them;
- Storage virtualization blends the physical storage of multiple devices so that it appears as a single resource pool;
- Network virtualization combines network resources and allocates their bandwidth as needed by a particular device or application.

### THIN CLIENTS, VIRTUAL DESKTOPS AND TERMINAL SERVICES:

Thin clients and virtual desktops represent alternative computing models that may offer advantages during a pandemic. Thin clients are small, inexpensive solid state devices with minimal operating systems. They connect to remote servers with a full operating system, applications and centrally stored data.

With thin client computing, upgrades and new applications are installed once at the server level, reducing maintenance time and effort, a significant factor if the ranks of IT workers are thinned. Additionally, widespread use of thin clients provides "single version of the truth," which could be helpful when coordinating an emergency response.

Virtual desktops disconnect the user's desktop from any specific device. Users can log onto their desktops on any available computer on the network. The server side can be configured to run many

desktops and applications in a shared environment resembling a thin client architecture, or can run each desktop as an individual virtual machine.

Microsoft Terminal Services and Citrix Presentation Server are the most common server-side technologies used to host multiple clients. Both represent a complex of services that allow applications to be controlled in one location (the data center), but run in many other locations.

**MOBILE APPLICATIONS:** Additional layers of technology support for responders are available in specialized mobile applications. Mobile resource management applications from manufacturers such as Utility Associates work in conjunction with existing asset tracking systems, providing enhanced information and unified views of resource distribution, even while both the user and the resources are on the move.

Mobile applications that work across multiple platforms and facilitate converged communications extend the communications infrastructure. For example, F4W's Energo Tactico software provides a gateway into a wide range of communications networks, including wide area, ad hoc, peer-to-peer, cellular, Ethernet, IP, wireless and VSAT (very small aperture terminal) networks.

As is the case with all the upgrades and implementations in preparation for a pandemic, these applications can and should be justified by their utility in normal operations as well. The dividend on disaster planning is improved daily operations and more effective handling of smaller problems.

## Unified Communications

Unified communications allows multiple types of electronic messaging and communications (voice, voicemail, e-mail, SMS, video, etc.) to be transmitted over a single converged network, and accessed through a single user interface on a wide range of devices. During a pandemic, UC capabilities will simplify the task of distributing critical information.

**EMERGENCY NOTIFICATION SYSTEMS:** Emergency notification of staff and responders is streamlined using unified communications because alerts can be transmitted simultaneously via an array of devices: computers, phones (VoIP, landline, cellular

or satellite), fax, PDAs, pagers or other handhelds. Alerts can be recorded and triggered via phone or the Internet. Messages can be targeted to groups or individuals, or pushed out to the public.

The ability to record and report message confirmation and response rates is an essential feature of these systems. Planners will need a near real-time view of how successfully information has been disseminated to anticipate complications in building closings or restrictions on transit systems, or to project the likely volume of citizens at prophylaxis centers. Notification systems that integrate easily into the larger information architecture will produce data that can be processed for rapid decision making.

**NON-IP NOTIFICATION SYSTEMS:** Every pathway to transmit information out to the public, the workforce and responders will come into play during a pandemic crisis. The most common non-IP notification systems are wireless or radio frequency (RF) alerts similar to those broadcast by the National Weather Service during weather emergencies. Specialized equipment is often required to receive these alerts, which limits their reach to the general public.

Other non-IP systems include those that generate mass automated phone calls delivering prerecorded information. Using electronic phone lists of organization workers, responders and the public (assembled from federal or local census information), these systems use automated PBX technology to dial through hundreds, thousands and even millions of numbers. They are generally programmed to make a specific number of attempts and to record the successful distribution rate of the message.

## Pandemic's Price

The most significant cost of a pandemic would be, of course, in suffering and lost lives. Almost as frightening in terms of widespread misery, however, are estimates that a massive H1N1 flu pandemic could cost the world economy as much as \$4.4 trillion, or 12.6 percent of global GDP, according to a recent study by ForeignPolicy.com.

**VIDEO SECURITY AND SURVEILLANCE (OVER IP):** Video security and surveillance technologies will act as force multipliers during a pandemic crisis, as they do during normal operation. Public safety and security personnel can be significantly assisted by extra sets of electronic eyes. In addition, specialized applications such as video recognition technology can be of help in access control.

Video surveillance in a circumscribed area usually involves cameras connected to a central data center either via wired or wireless IP Ethernet connections. Mesh networks can be used to push the geographic range of video surveillance.

In this scenario, signals are delivered to and from remote cameras via a mesh of access points, which can then be joined to the unified IP Ethernet network via root access points. From there, video from the cameras is available to devices on the network, with mobile remote access possible within the range of Wi-Fi signals.

## Asset Management

Effective asset management systems are the foundation of resource accountability. More importantly, in a public health emergency, asset management will help ensure that equipment, medicines and supplies will be deployed where they are most needed. Appropriate provisioning of mass prophylaxis and treatment centers will depend on systems that match real-time information about the needs of any specific site with resources that can be dedicated to it.

**ASSET TAGGING AND TRACKING:** At the most basic level, asset tagging and tracking simply involves affixing a tag or label that contains key information, minimally a serial or product number, to a physical asset. Lists of that tag information are then used to track the location of the asset, usually retrospectively, through processes that are frequently paper-based and labor-intensive.

Barcode labels represent a huge step toward automating asset and inventory tracking. Barcode readers can feed data directly into management software that lets the organization know what assets are available, where they are and where they might be needed. Tagging and tracking systems that are based on barcode labels have the advantage of being familiar (nearly ubiquitous) technologies that are relatively inexpensive compared to RFID technology.

A significant consideration in pandemic preparation should be the interoperability of asset tagging and tracking systems. Government resources are already tracked by law, and most NGOs or private partners will have systems in place to keep track of physical assets. Valuable response time can be lost while mobilizing those resources if the systems operate in parallel rather than intersecting effectively.

**RADIO FREQUENCY IDENTIFICATION:** RFID technology tracks physical assets using tags and readers, each of which contains both a radio receiver and a radio transmitter. RFID tags (which can be

manufactured in almost any size or shape) are fastened directly to assets or shipping materials and are programmed with information about the resource. Some RFID tags are powered by batteries, while in less costly versions of the technology the tags are activated and powered by signals from the RFID reader.

RFID tags are available in read-write, read-only and "write once, read many" versions. Read-write chips allow users to add information to the tag or write over existing information when the tag is within range of a reader. Data gathered by RFID systems can be fed directly into asset tracking software, automating the tracking process almost completely.

Reading ranges of RFID systems vary with radio frequency: up to one foot for low frequency systems, up to three feet in high frequency systems and up to 20 feet in ultra-high frequency (UHF) systems. Standards are emerging for UHF systems, making them more attractive for supply chain applications, and this could make RFID tagging more valuable as part of the response to a pandemic.

## Data Storage and Power Management

One certain consequence of a pandemic will be the creation of massive amounts of data — statistics about outbreaks and the spread of the disease, health records from prophylaxis and treatment centers, information about the location and availability of resources, and much more.

That flood of information will need to be gathered and safely stored in a way that makes it readily available to planners and responders trying to keep ahead of the emergency.

**DATA STORAGE SOLUTIONS:** Storage area networks (SANs), and to a lesser extent, network attached storage (NAS), are central to any data storage strategy, especially for large organizations. SANs link multiple storage devices and present them as unified resources to users. Individual SANs provide scaleable storage and multiple SANs can be linked to provide a larger repository.

Storage can also be virtualized at the server, device array or SAN level. Virtual storage offers cost and space savings and easier management of the pool of storage resources.

Especially at a time of heightened stress for an organization, a complete data storage solution should include the following (mostly automated) functionality:

- A document capture and management system to digitize paper-based information and move it from physical to electronic storage;
- Backup software that automates the process of moving a copy of data onto appropriate storage media so that users can recover lost, deleted or corrupted files;
- Replication software that creates an electronic copy of data in another location for use in disaster recovery;
- Archiving software that systematically classifies data and divides it according to criteria such as need for availability, lifecycle, legal requirements and policy mandates.

**ACCESSING AND SHARING DATA DURING A PANDEMIC:** Preserving data in storage is only half the job. Decision-makers must be able to retrieve the information and share it. Recent surveys show that, after security, the ability to access data quickly and easily is often the most common concern about storage technologies among IT professionals.

## Old-time Tech

Despite the rapid pace of technological change, much of the physical asset management happening today is based on barcode systems, which were invented in the 1950s and had appeared in supermarkets and distribution centers by the 1970s. RFID is even older, having its roots in technology developed by the British to identify friendly planes during World War II.

Online storage (hosted services that operate in the Internet cloud) is an option for some stored data, but most government entities will maintain an in-house storage infrastructure. The key to accessing stored data will be the software management system. A crucial consideration during a pandemic is the ability to push an access interface out to nontechnical workers.

**POWER PROTECTION AND MANAGEMENT:** Unlike a hurricane or earthquake, nothing in the nature of a pandemic threatens either the local or regional power supply. The health emergency is, however, likely to reduce the number of utility and IT professionals available to cope with an outage.

A best practice is to back up your systems with uninterruptible power supply (UPS) systems, devices that provide battery power when electricity from the grid or a generator is not available.

Several factors should be considered when selecting a UPS solution. Most basic is the present level of power consumption, both for the entire operation and for key segments. Add to that calculation the impact of any planned initiatives or projected growth on power consumption in order to choose a UPS that can handle the capacity needed.

Runtime, or the amount of time the UPS will provide backup power for systems and devices, should also be a consideration. All but the most basic UPS solutions have integrated software that provides management features, including monitoring the system remotely.

## Manufacturer Options

**SONICWALL** is a manufacturer of Internet security solutions. SonicWALL SSL VPNs offer secure remote access to mission-critical resources from virtually any endpoint, including desktops, notebooks, PDAs and smartphones. The manufacturer provides a broad range of scalable VPNs to meet the needs of organizations of all sizes.

**VMWARE** is a leading manufacturer of virtualization software. VMware Server is a hosted virtualization platform that installs on any server and partitions the physical server into multiple virtual machines. The virtual architecture created by VMware Server can be managed using VMware vCenter. VMware's vSphere is the IT industry's first cloud operating system and is designed to deliver IT infrastructure as a service.

**F4W** makes mobile communications solutions based on its Energo framework. Energo Tactica 2.0 is a convergent communication application that bridges wireless-capable devices and software communications solutions. Energo Tactica enables access to a wide array of application functionality across ad hoc, peer-to-peer, wide area, cellular IP, Ethernet, wide area wireless and VSAT networks. Besides being one of the most cost-effective solutions in the market, Energo Tactica is designed for ease of use by nontechnical staff.

## Telework Checklist

Here are some steps the IT team can take that will smooth work staff transition to teleworking before a pandemic strikes:

- Ensure system security and stability;
- Make operational information web-accessible;
- Enable remote access systems;
- Transition staff whose work best suits telework first;
- Develop a culture migration plan that enables the workforce;
- Define new metrics that reward and guide teleworkers.

Source: Cisco

**UTILITY ASSOCIATES** makes solutions for mobile asset management. AVail is a highly secure command-and-control solution that provides an automatically updated, near real-time view of the current location and status of mobile assets layered with information from core business systems. OnComm Rocket is a device that enables an organization to track the location and status of virtually any mobile asset, from toolboxes and backhoes to personnel and vehicles, in near real time.

**CISCO** is an industry leader in IP telephony and unified communications, offering a wide array of UC software and services and its Unified Communications Management Suite. Cisco's UC offerings enable the workforce to communicate with a combination of voice, video, data and mobility applications across multiple workspaces. In addition, Cisco WebEx provides a powerful platform for remote collaboration and virtual meetings.

**EMC** is a manufacturer whose central focus has been storage and information management solutions, but the company manufactures an extensive variety of other hardware and software solutions as well. EMC CLARiiON AX4 and EMC Symmetrix are networked storage systems that can be used to consolidate data into a single pooled resource and which support VMware storage virtualization.