



# Lippis Report

White Paper

Lippis Report 132:  
**Mitigating Pandemic-Caused  
Business Outage With Teleworking**

by  
Nicholas John Lippis III  
President, Lippis Consulting

September 2009



## Lippis Report 132: Mitigating Pandemic-Caused Business Outage With Teleworking

The World Health Organization (WHO) has reported over 182,166 laboratory-confirmed cases of 2009 H1N1 influenza virus with 1,799 deaths. In June 2009 the WHO raised the pandemic alert level to six, signaling a pandemic of this influenza is underway. If the H1N1 virus, or swine flu, is in full pandemic force during the fall and winter months of the seasonal flu, 40 to 50 percent of the workforce could be affected; yes that's 40 to 50%. However, early numbers indicate H1N1 is no more infectious than seasonal flu strains that typically hit each year. But H1N1 could still pose a significant threat. New flu strains can mutate, sometimes becoming more serious and more contagious. Businesses may have already been impacted by the spring and summer outbreaks of 2009 H1N1 influenza affecting their employees. CDC anticipates that more communities may be affected than were in the spring/summer 2009, and/or more severely affected, reflecting wider transmission and possibly greater impact. In addition, this fall and winter seasonal influenza viruses may cause illness at the same time as 2009 H1N1.



### Mitigating Business Outage With Pandemic Planning

[Listen to the Podcast](#)

The severity of illness that 2009 H1N1 influenza flu will cause (including hospitalizations and deaths) or the amount of illness that may occur as a result of seasonal influenza during the 2009–2010 influenza season cannot be predicted with a high degree of certainty. Therefore, employers should plan to be able to respond in a flexible way to varying levels of severity and be prepared to refine their pandemic influenza response plans if a potentially more serious outbreak of influenza evolves during the fall and winter. More people and communities are likely to be affected as influenza is more widely transmitted. While H1N1 provides the immediacy of action, business disruption on this scale can occur due to multiple causes. Virus outbreaks or other natural disasters, man-made disasters plus major events such as protests or large scale national strikes common in some European countries are all potential causes of workforce disruption. Note that multiple events can and do occur simultaneously amplifying the total impact of these events on businesses.

So the question to business and IT leaders is this: what if 40 to 50 percent of your workforce cannot get into the office? Are you prepared? According to Gartner only 13 percent of enterprises are prepared for a major workforce disruption where employees cannot travel to the office. For IT leaders a best practice to minimize the impact of a workforce disruption caused by a H1N1 pandemic, another infection, man-made or natural disaster is a scalable, secure and reliable teleworking solution.

### Secure Teleworking Access

Pandemic mitigation is best addressed with remote access technologies where physical IT assets are still intact but mobility has been restricted and in some cases drastically restricted by quarantining. A close cousin to pandemic planning is business continuity planning. During a crisis business and IT leaders first usually start thinking in terms of connectivity, meaning how to connect voice, video and collaborative application resources to remote workers when office access is highly restricted. Unfortunately, if business and IT leaders are thinking in this way, they often overlook secure access as their knee jerk reaction is just to connect employees. When IT leaders are responding to a pandemic and executing their plans with remote access to applications and collaboration, remote workers workflow security should not be compromised as it is most vulnerable at this time. To ensure remote access to IT resources and communications are secure, security technology needs to be systemically embedded in the remote access solution from the client software to the routers to the applications.

**Cisco OfficeExtend**

[Get the White Paper](#)



## Role-Based User Configuration

In addition to secure access and connectivity, policy over the use of this business continuity resource is important to ensure that different job functions, responsibilities or roles are appropriately administered. What this means is that the management system should allow configuration of user profiles with associated privileged access to business assets. For example, there are employees who will perform their duties at a home office while others who are mobile conduct a large percentage of their business on smartphones. These two examples represent different device, connectivity and security needs. Therefore, a pandemic teleworking solution should be flexible to support multiple user scenarios, needs and employee roles.

**TLS Proxy and Phone Proxy for the Cisco ASA 5500 Series**

[Get the White Paper](#)

## A Framework for Preparedness

A best practice framework approach to business continuity planning includes policy definition and IT preparedness. While assessing business risk for workforce disruption, IT leaders should work with Human Resources to categorize employees by responsibilities, into groups of communications and application requirements and job roles. This is helpful in defining user roles and policy so when a crisis hits IT can execute a plan defined during a period of calm. While this work is underway IT leaders should survey existing remote access solutions and network capabilities with the goal of identifying gaps that need to be closed considering the potential that 40 to 50% of the employee base is forced to work remotely.

When surveying the remote access solution, six items are recommended for consideration. First, review access methods and connectivity options available for each remote access scenario. For example consider mobile devices, laptop and notebooks and even public kiosks as power outages may force employees to public spaces for enterprise connectivity. Second is the level of access, meaning employees/partners/contractors should receive different levels or priority of access. Third is to consider security technology essentials, primarily firewalls, virtual private networking (both SSL and IPsec) and Network Access Control for granular user and end-point access to networked resources. Fourth, voice, video and data connectivity need to be considered during pandemic crisis to assure IP and TDM phones, softphones and collaboration software are functional as these will be the tools executive management and others rely upon when travel to the office is not an option. Compliance requirements such as PCI, FISMA, SOX, HIPAA, Presidential Directives, et al., need to be considered as their non-compliance can result in serious penalties to executive management. Finally business recovery, while often overlooked is an important practice to restore business and IT assets after an event.

## A Remote Work Environment

To ensure business operations during and after a displacement event, a remote work environment only needs to be based upon a few technology pillars including virtual private networking for connectivity, VoIP for voice communications, conferencing and collaboration software for video and virtual meetings plus embedded security. With these pillars a robust and resilient pandemic response plan can be executed which exhibits these attributes.

**Wide & Resilient Access:** Extend connectivity to employees working remotely. During a displacement event connectivity needs to stretch across a variety of end-points, such as company-provided and employee-owned PC/laptop/notebook, public internet terminals and/or internet-enabled mobile phones. Connectivity needs to scale up to support a burst of employees, as high as 50% of the employee population, displaced and thus attempting to access corporate IT assets from a wide geographic area. In addition, the remote network access facilities supporting teleworkers and mobile users should be geographically resilient as well, with back-up access equipment at different sites to ensure availability in case a site is disabled or destroyed due to the displacement event.

**Real-time Communications & Collaboration:** To ensure workflow and business process keep moving, real time communications and collaboration services are required. In most cases a computer/laptop is all that is needed for the employee to stay connected and productive with unified communications and collaboration software such as webex.

**Embedded Security:** With policy defining user roles and configured into a teleworking management system, IT will be able to provide access to corporate assets based upon roles, access medium and end-point. In addition, with firewalls, tunnels and network access control IT has the tools to mitigate cyber threats that often accompany pandemic and other workforce displacement events.

**Centralized Management:** Teleworking or remote access solution are characterized by a few IT personnel offering network service to a large number of people dispersed over a very large geographic area which is often challenging and costly to administer, thanks to a ratio of 1 IT ops to 20,000 teleworkers. Network management is the only tool IT has to manage this ratio and contain cost while delivering an excellent teleworking experience to the employee. Therefore, centralized network management including configuration, change management, etc., which the employee does not need to touch, is key to successful large scale teleworking solutions.

### The Cisco Teleworking Solution Set

There are many providers of teleworking solutions including Cisco Systems, 3Com, Juniper, Avaya, Mitel, NEC, Siemens, et al. But there is only one company that offers solutions that deliver networking, communications and collaboration with embedded security. That company is Cisco. To address this market, Cisco has introduced a solution portfolio. Depending on a customer's needs, teleworking usage profile, or security requirements, Cisco has solutions that combine technology and services to deliver an integrated approach.

For example, the Office Extend AP is designed to provide secure, corporate wireless to the home office user or road warrior in a small access point form factor. The Cisco Adaptive Security Appliance (ASA) supports secure remote access not just through SSL or IPsec VPN, but also a phone proxy feature that works to secure voice traffic direct from an IP phone. And finally, the Cisco Virtual Office (CVO) is a solution designed for premium teleworking services including single-number reach, a dedicated multiservice platform for tighter security, and zero-touch management. CVO also supports dual mode phones extending solution flexibility to secure mobile infrastructure.

Think of Cisco's approach this way: different end-points and access methods create different user experiences. Cisco's teleworking solution supports a broad range of experiences such as workers accessing corporate assets securely from public spaces such as a coffee shop computer, in the confines of their home or on the road. Each one of these scenarios has different security requirements and capabilities which the ASA and or CVO serve up to remote and mobile users. In addition all of this is centrally managed and configured which frees up employees to simply be productive.

In addition to the technology, Cisco offers a flexible licensing option which allows organizations to scale up their VPN usage to that 40 to 50% of employees without the need for new equipment but only a management key to unlock as many VPNs as needed during a pandemic or other dislocation event. As a reference, on average only 10% of an employee population has regular access to VPNs, but as many as 50% may need access during crisis. Cisco's shared licensing option means that licenses are no longer attached to a single location. For example, a 10,000 user license could be shared among different locations and employees providing elasticity of VPN availability through a licensing arrangement to accommodate the surge in VPN requirements during pandemics or other disasters.

No one wants to manage through a crisis, but those that plan now will find that successful crisis management is not only good business but a career booster as well. Many executive managers find that they are granted greater responsibility and stature after successfully guiding their corporation or government through a crisis. With the autumn approaching fast and the potential for a H1N1 outbreak, now is the best time to position your company to both respond to a pandemic and recover from its damage. A teleworking solution is can be a major component to that plan.