

# Everything But Contingency Planning

## Abstract

Anecdotal evidence strongly suggests that businesses today are not spending sufficient information technology money on risk management activities. This is especially true with small and medium sized organizations of fewer than five hundred employees. The purpose of this article is to identify technology projects that are not, strictly speaking, contingency planning projects, but that will create contingencies as a side benefit. We will bypass the subject of business process identification in favor of end-result improvements in remote connectivity, communications, network availability, and the paradigm change associated with telecommuting initiatives. These improvements are categorized into five projects that an organization might consider acting upon. Our hope is that smaller organizations, which might normally do little to plan for continuity of operations, consider these improvements not only for business continuity and recovery purposes, but also for the value of the project itself.

## Introduction

Especially in a down economic environment, (including the present one), it is difficult to appropriate dollars for contingency planning activities. Many Chief Information and Technology Officers (CIO/CTO) now operate on a shoestring, with barely enough to cover normal operating expenses. New technology initiatives are under intense scrutiny, and the lifecycles of existing systems continue to expand beyond industry standard replacement recommendations. Management asks information technology to do more with fewer resources. It is no surprise that risk management activities take a back seat to daily operating expenses.

Contingency planning is a broad category of IT risk management normally divided into four categories. A *Business Impact Assessment (BIA)* is a planning document that aims to identify vulnerabilities and threats to business processes. A *BIA* prioritizes corrective action and other protection planning to those systems that matter most to an organization. An *Incident Response Planning (IRP)* document strategizes how management should best respond to various incidents of concern. A *Business Continuity (BC)* document discusses how an organization can continue to run its most critical operations, in an alternative location, if and when the primary organization is unavailable during a disaster. A *Disaster Recovery Planning (DRP)* document lays out the steps an organization should follow to fully recover operations in the event of a disaster (Whitman, 2007).

Every organization's *BIA* and *IRP* are as unique as its business processes. A quick search of the internet will identify software applications and templates that may serve as a springboard or starting point to the planning process, but the hard work cannot come from a template or software program. However, certain aspects relating to the continuity of operations and disaster recovery processes can directly benefit from savvy network acquisitions that are not strictly defined as contingency planning activities.

The purpose of this article, "Everything But Contingency Planning", is to identify everyday projects and planning that seemingly have little to do with contingency planning, yet when implemented with contingency planning in mind, have a large net effect on it.

## Project # 1 – Implement VoIP telephony.

Is your phone system breaking down? Is your phone system lease over? Voice over IP (VoIP) telephony is well known for leveraging the internet to reduce the cost of phone calls. While this is certainly true, VoIP has functionality that assists in incident response and business continuity planning.

The first benefit is remote and soft phone functionality. Remote phones are VoIP phones that operate outside the main office facility. They function just like normal office phones. Staff can dial by extension, and the user still enjoys the same application functionality, such as voicemail and conference calling services. Many telephony providers are simplifying the configuration of remote phones by building virtual private network (VPN) client software directly into the phone. A soft phone is an application loaded onto a remote computer, such as a laptop, that can leverage a headset to function as a phone. Soft phone applications might have an image of the actual desk phone as part of the application to assist the user and make the solution more user-friendly (Cisco Voice and Unified Communications, 2009).

Four strategies are commonly used for voice contingency planning purposes, as they relate to the use of remote phones. First, phones can be implemented in the homes of certain key employees. Management would know that in the event of an incident, these employees would be able to use their desk phones with their existing office extension, known as a bridge line appearance. This would allow staff to communicate with key customers, suppliers, and other employees. The disadvantage is that this solution offers little flexibility. In the event of a disaster, only the preplanned users can take advantage of the remote communication plan. As a second option, phones could be available in a stockpiled location. This would allow an on-demand and incident-specific deployment of phones. This solution requires more reaction time, but offers greater flexibility in how the business allocates phones in the event of a disaster. Finally, the organization might elect to deploy phones in a warm or hot disaster recovery site. In a warm scenario, phones could be programmed, and then boxed, ready for use in the event they are needed. In a hot scenario, the phones would be ready to go, and the communication lines required to support connectivity would be ready to go on day one.

The second technology advantage of VoIP phones is a service called “find-me/follow-me”. Phones are set up to route calls based on a predetermined set of rules. A sales person can configure routing so that all calls ring a dedicated desk line first, a cell phone second and perhaps a home office last. Organizational leaders have hailed this application as a great gain in efficiency. More calls are answered on the first attempt, instead of voicemails logged for later attention. The client receives immediate attention, and is presumably happier. From a contingency planning point-of-view, this service allows callers to route to phones that are outside the corporate office. This might prove critically important in the wake of an incident that does not allow staff to enter the office building.

The third technology with VoIP is phone system hosting. There are many carriers that offer a “hosted VoIP” solution for small and medium sized businesses. The core phone system resides in a carrier-grade facility, with only IP (phone) handsets deployed to the desks of the users. If a disaster occurs at the corporate office, only new handsets would be purchased and installed in an alternate location. The core “phone system” would remain operational, configured, and ready to go. In fact, if a customer were to call, the automated attendant would continue to operate, as would voicemail services and “find-me/follow-me” functionality. It is fair to say that communications would continue to occur in a temporarily degraded capacity, as a result of the secondary contact point.

Finally, many VoIP systems are implemented with a failover function. Cisco’s phone system, for instance, has a feature called survivability that allows its VoIP systems, called Call Manager, to failover between locations on a wide area network (WAN). A savvy network manager might implement a small phone system in a secondary location, so that it could failover for the primary office in the event of an outage (Cisco Voice and Unified Communications, 2009).

In summary, there are many reasons why you might implement a new phone system. Contingency planning certainly isn’t a driving reason behind such an expensive purchase. However, if you are looking at an implementation, you should strategically orient your telephony acquisition to improve continuity of operations. The four key aspects of VoIP as they pertain to contingency planning are:

1. Use remote phones and soft phones to extend the reach of your phone system outside your main office building.

2. Use call routing technologies, such as “find-me/follow-me”, to allow clients and vendors to reach you in the event of an incident.
3. Smaller organizations can host their phone system with a carrier. This has built-in business continuity implications.
4. Fail-over your phone system to a secondary location using technology such as survivability.

## Project # 2 – Start an employee telework plan.

Telework plans make sense for many reasons. Offering this flexible work environment might make your organization more attractive to a wider base of potential employees. Telework frees up work space and other resources of the traditional office building. Certain studies have also concluded that employees accomplish more and work longer hours for the employer in a telework environment. This is likely a product of spending fewer hours in the car commuting every day.

All of these are solid business reasons a telework plan might help your business efficiency. It might also assist with continuity of operations in the event of an incident as well. Instead of relocating staff to temporary work space as part of a business continuity plan, an organization that invests in technology for telecommuting might have created a fully-functional “virtual” telework environment without realizing it. The following five technology purchases will have you well on your way.

First, implement a virtual private network (VPN) appliance to establish secure remote connectivity. VPN devices allow remote computers to connect to the corporate local area network (LAN) from any internet connected device. The connection is encrypted between the two points for security of data transmissions (Clarke, 2009). Additionally, the VPN device can map network shares, allowing simple access to corporate data via a traditional drive letter mapping. Though many firewall devices can also perform VPN function, be mindful of the load created on the device (Ingham, 2002). Handling a few users concurrently is vastly different from hosting VPN connections for an entire staff.

Second, consider using laptops for staff instead of desktop computers. Corporate issued laptops allow a controlled environment where the VPN software and other utilities are preloaded and ready-to-go. With the computing power in hand, the viability of a remote computing initiative is more feasible than using a wide variety of home computer or public “kiosk” computers. Additionally, the cost of laptops computers continues to decrease to the point of justification in almost all organizations. A good corporate laptop can be purchased for less than a thousand dollars.

The third recommendation is to implement cell phone data tethering. With the majority of organizations issuing smart phones, such as Blackberry devices, Windows smart phones, and of course the iPhone, the buyer purchases data connectivity along with phone minutes. This data connectivity is used to access email and surf the internet. It can also be used as a makeshift internet connection on your laptop computer. A small application is installed on the target computer. The application establishes a connection from the phone to the laptop computer, and allows the computer to use the phone’s connection to the internet. The user can now connect to the corporate VPN and access other related services.

The implementation of Microsoft terminal services is the forth recommendation. Terminal services are a Microsoft server-based application that run under current server environments such as Windows Server 2000, 2003 and 2008. Terminal services run a copy of a network application remotely (Microsoft Remote Desktop Services, 2009). For instance, a corporate implementation of email, accounting, or sales management software would be accessible over the internet with Terminal Server. This remote connectivity to critical line of business applications is a core component of an effective telework plan, and is equally important in a business continuity situation.

The fifth and final recommendation for creating a telework technology environment is to load test and document application usability. Pick a Saturday and ask staff to participate in a load test of the remote access system. Often overlooked, this last step is a critical component to verification that the new remote access system is capable of handling the load of a full staff. Performing this step confirms that your remote access system can be leveraged as a business continuity tool. In summary, the five key technological aspects of an effective telework plan are:

1. Implement a VPN solution that provides secure connectivity into the corporate network from any internet connection.
2. Issue employees laptops rather than traditional desktop computer systems.
3. Install tethering software so that cell phone users can leverage internet access for makeshift internet connectivity on their laptop computer.
4. Acquire and implement Microsoft Terminal Services to host remote access to corporate applications via an internet connection and VPN tunnel.
5. Test the remote access solution against the full load of staff. Ensure that your system can accommodate full staff in the event of an incident.

### **Project # 3 – Purchase collocation space in a third-party datacenter.**

For most organizations, a tier-four datacenter supplies an environmental setting that cannot be duplicated cost effectively by an individual company. Datacenter space offers redundant power (typically from separate carriers), battery backups, long-term power by generator in the event of power outage, security, and building design making is less susceptible to natural disaster, as well as a host of other benefits (designDATA datacenter services, 2009).

In short, it is likely that a datacenter will be available and running your equipment twenty-four hours a day, when you need it most. With the oversupply of broadband connectivity created in the early 2000's, many organizations have found that they can collocate equipment in a datacenter facility, and leverage fiber communication resources needed to establish a secure connection between the corporate home office and the datacenter facility.

The initial business case for collocating equipment in a datacenter varies. The following events are predictors for a possible move to datacenter services.

- Your organization recently lost power or internet connectivity for an extended period of time.
- A new customer facing, internet-based application deployment threatens to expose availability concerns within your environment. Management decides to host this application in a carrier grade facility.
- Network availability concerns identified during an audit or assessment.
- A generator or air handler failure costs too much to repair. The customer elects to move systems to another facility, and forgo the initial capital outlay for repair.

In summary, moving equipment to a datacenter, though an additional ongoing cost, provides a better environment than an organization could develop on its own, and is more likely to be available even in the event of a significant natural disaster.

### **Project # 4 – Begin using server virtualization.**

Virtualization is a technology that allows multiple servers operating multiple software instances to run on fewer physical servers. Advanced versions of the virtualization software also allow servers to operate in resource pools and share resources. Think of many servers acting as one large grid of servers. The net

result is the formation of a redundant processing pool of power. (VMware Server & Datacenter Virtualization Products, 2009) In the event a server fails, its counterparts will manage the load until the failed unit is back in service.

This configuration requires a dedicated storage component called a storage area network (SAN). This SAN is the heart of any server virtualization engine. In this configuration, the servers themselves are leveraged for their processing power, and the SAN actually contains all of the storage, for all of the servers, in one location. All mid-range and enterprise storage manufacturers sell replication engines that allow SAN devices to replicate to a counterpart. In certain cases this second device might be local (in the same physical location as the primary). For disaster recovery purposes, a savvy network engineer might recommend that the SAN reside in a secondary location, such as a datacenter, so that this data is physically outside of the primary premises. In the event of a disaster this would safeguard the data. Extra servers can connect to the second SAN completing the stand-by environment (VMware Server & Datacenter Virtualization Products, 2009).

In short, SAN to SAN replication, combined with virtualization, provides a short-path to a warm disaster recovery site, and is surprisingly similar to a hot-site, ready to take over as the production network when needed. In summary, the steps required to implement a server virtualization plan that lends itself to a warm site replication include the following:

1. Purchase several like servers with dual processors and 32gb of memory or greater.
2. Select enterprise virtualization software, such as VMware vSphere or Citrix Xen.
3. Implement a dedicated storage area network.
4. Purchase a second storage area network and replicate data between the two.
5. Use spare or older servers in a secondary stand-by capacity and connect to the second storage area network.
6. Test failover.

## **Project # 5 – Write a plan that addresses H1N1 response.**

With the advent of the H1N1 virus, organizations world- wide are deeply concerned over possible business-related consequences in the event of a global pandemic. One major concern with this virus is the quarantine process. As we've seen in the past, the government may react by closing down public areas, such as school systems, to prevent the further spread of the virus. This will have a trickle-down effect as employees may need to stay home to care for children, or may be sick themselves. Mass transit, such as the local metro line, may be unavailable. The possibility that an organization would need to continue operations with a skeleton staff is a real one.

In this set of circumstances, a communications and response plan that addresses what to do in the event the physical company offices close would be invaluable. It would also lay the foundation for a larger incident response plan that covers different vulnerabilities.

Focus the plan on communication between management and employees, and the continuation of the most important business processes (Kairab, 2005). Can you still process orders, communicate with clients and key vendors? Can you process payroll and deposit checks? Concentrating efforts on the most critical processes will focus the planning effort to a manageable set of processes.

## **Concluding Remarks**

Too often the industry behind contingency planning creates a cloud of confusion around risk management and contingency planning activities. This confusion manifests itself in a belief that contingency planning

initiatives are too costly, cumbersome, and inappropriate for organizations of a smaller size. Truth be told, often the most difficult part of the process is simply getting started. We have made no attempt here to discuss what most risk management firms would consider the starting point in this endeavor, the identification of business processes, associated risks, and corresponding vulnerabilities. The intent behind this is not to diminish their importance. Rather, by looking at risk management activities in the light of technological improvements which are likely to occur regardless, we may have improved the likelihood of a smaller organization proactively considering, and more importantly acting on, this critical topic.

Therefore, this article is a simple one. Five actionable ideas for improving a technology posture, while aiding in the continuity of business operations along the way. If you have any questions, the author's email address is [mruck@designdata.com](mailto:mruck@designdata.com).

## References

(2009, December). Retrieved December 2009, 2009, from designDATA datacenter services: <http://www.designdata.com/technology/data-center/>

*Cisco Voice and Unified Communications*. (2009, December). Retrieved December 2009, from Cisco : <http://www.cisco.com/en/US/products/sw/voicesw/index.html>

Clarke, J. (2009). Resilience under attack: Techniques for continuing online business in the face of security compromise. *Journal of Business Continuity & Emergency Planning* , 3(3), 222-226.

Ingham, K. F. (2002). A History and Survey of Network Firewalls. *The University of New Mexico, Computer Science Department* , 1-42.

Kairab, S. (2005). *A practical guide to security assessments*. Boca Raton: CRC.

*Microsoft Remote Desktop Services*. (2009, December). Retrieved December 2009 2009, from Microsoft 2008 R2: <http://www.microsoft.com/windowsserver2008/en/us/rds-product-home.aspx>

*VMware Server & Datacenter Virtualization Products*. (2009, December). Retrieved December 2009, from VMware: <http://www.vmware.com/products/datacenter-virtualization.html>

Whitman, M. E. (2007). *Pricipals of Incident Response and Disaster Recovery*. Massachusetts: Thomson Course Technology.