17

TELECOMMUNICATIONS AND NETWORKING

Your Connection to the World

Everything is connected . . . no one thing can change by itself.

—PAUL HAWKEN

INTRODUCTION

All of us are interconnected, as people and companies. We use data networks to connect to suppliers, customers, business associates, and friends. Data communications has enabled our businesses and personal lives to be "just in time," no matter where we might be in the world. We use data networks to talk, share data, run applications, download files, organize schedules, exchange email, and access the Internet. We use these networks to connect us with our coworkers and to collaborate with customers. This chapter reviews the dangers that threaten our data networks and the attributes unique to these networks that require special processes to restore them after a disaster.

Some organizations have two distinct networks: one for voice communication that uses the standard telephone system (also known as the public switched telephone network, or PSTN) and another for data communications that uses one or more computer networks that are typically connected to the Internet. The need for two distinct networks is rapidly fading with the increasing use of Voice-over-Internet Protocol (VoIP) for sending voice communications over the Internet. Some organizations will maintain both networks for the foreseeable future. Fortunately, both types of networks have similar issues that simplify disaster recovery planning.

PUBLIC SWITCHED TELEPHONE NETWORK

How important can a telephone line be? What's the cost of a telephone call? What is the value of a missed call? How much would you pay for 100 percent telecommunications reliability? Is such a thing even possible?

Consider this scenario. You are the Materials Manager for a major factory, sitting at home in your living room. As you watch the evening news, you see a video of flames rising out of the roof of a key supplier's main factory. You don't need trouble like this. What should you do? Without a steady flow of materials from this supplier, your factory could be idled and customers lost. You try calling your salesperson and the supplier's company offices but no one answers. First thing in the morning and all the next morning you try calling them. The company is more than two hours' drive away and you cannot get away from the office for that long. Your calls still go unanswered.

Looking through your contact list, you select another supplier and place an order for a two-month supply of goods to replace the supplier that had the fire. The setup costs are a killer, but it is worth the money if you can keep your assembly lines running. At least this problem is contained. Trouble is, the fire you saw on TV was isolated to the front offices and the factory is fine. The supplier's warehouse is bulging with finished goods. At a time like this, the supplier needs the cash, but employees can't call out until the telephone switching room is replaced! The supplier's efforts focused on recovery from the fire but forgot all about its customers.

All companies strike a fine balance between the cost of reliable telephone service and the cost of downtime. In a time of tight budgets (which is always), you balance the cost of premium services against the potential loss of telephone service. The more resilient you want your telephone network to be, the more money must be spent. Telephone service is central to the conduct of business in most companies. A failure isolates customers and suppliers from your company —and that can quickly become a very lonely feeling.

Some companies are even more dependent on telephone service than others are. If you work at a factory, a telephone is used to conduct business, but the main concern is moving products down the assembly line. The loss of telephone service does not slow down the facility's production one bit. However, if your facility is a call center for sales or service, then 100 percent reliable telephone service is crucial to your ongoing business. In the factory example, if the conveyor on the main assembly line breaks, the workers have nothing to do. In the call center, if the telephone service is interrupted, then they are likewise idled.

The North American telephone network is designed to carry traffic from about 10 any better because portions of it also use landlines and it has its own capacity limits.

The high level of telephone communications reliability of our modern telecommunications networks is the envy of the world. The disasters that may befall your delicate communication lines are legion. Anywhere along the network's path the wire can be broken, switching equipment can lose power, or problems can even occur within your building. Ensure that your company has reviewed the risks to its telecommunications pipeline and has taken steps to reduce the likelihood of failure. Our job here is to identify those risks and build a wish list of mitigation actions to make your company's telephone communications even more rock-solid than ever before.

PSTN BASICS

The world of telephonic communications begins with an end-point, the telephone instrument on your desk. This modern marvel connects you to the world at large. The telephone is connected by wire to the wall jack, which in turn is connected to a wiring closet. A wiring closet may be one of those locked doors on your office building floor that you never get to look inside. The same function can be served by running wires to a specific place on the wall of a factory (which is generally a wide-open space). In either place, you would see brightly colored wires running in spaghetti-like fashion to a telephone wire "punch-down block" or punch block.

If you look at a punch block, it seems to be a "rat's nest" of colored wires routed in an orderly fashion yet going in all directions. Each office telephone has at least one pair of wires running from its wall jack all the way back to the wiring punch block. The punch block also has wires running to the telephone switch for your building. This is where the two are connected to each other.

PRIVATE BRANCH EXCHANGE

From the wiring closet, large bundles of wires run to the company's telephone switching equipment. In a larger company this would be a Private Branch Exchange (PBX) device. A PBX replaces the long-gone company telephone operator who would connect internal calls with a plug patch panel. The patch panel physically connected the wires from one telephone instrument into the wires of another. This is a basic operation, but until electronics matured, it was the only way to do it. It is now all done electronically. In today's offices, a PBX takes these incoming wires and, using the signal on them, provides electronic routing of calls within the building. Think of a PBX as a special-purpose computer with all the support needs of a computer server.

The PBX determines which calls are intended for external telephone numbers and connects to the local telephone company central office using "trunk" lines. Trunk lines are used for inbound or outbound calls. The number of trunk lines the PBX has connected to the central office determines the maximum number of external (inbound or outbound) calls you can support at a given moment. Modern PBX systems offer a wide range of additional services such as:

- Voice mail
- Telephone conferencing
- Call transferring
- Music on hold

As a result, from a business continuity perspective, you have a large single point of failure device. You must plan to recover from a catastrophic failure of the PBX (e.g., burned to a cinder in a fire). A close examination of the PBX room and its ancillary equipment will show that it is essentially a computer room, requiring the same electrical and climate stabilization actions as any computer room. Backup copies of the configuration data must be made for each device and handled with the same care as the backup data from your computer system. The data should be securely stored off-site and available when needed. Up-to-date backed-up data is the key to a prompt recovery.

Internal to a company, the telephone signals can be analog or digital. Digital PBX systems provide a wide range of services beyond simply routing calls. Most PBX systems use digital signals to communicate with the telephones. This allows for additional services, such as one-touch dialing, preprogrammed telephone numbers, and voice mail, which is significant in the case where you want to use a modem to dial out of the office. A fax machine or a direct modem connection requires an analog line. If you have a digital PBX, then you will need separate analog lines.

Rather than run a multitude of analog telephone lines, most companies access the Internet via their external data network. This works fine for most office dwellers. However, some special-purpose devices still need these analog lines and you should keep track of where they are. Examples of analog dial-out lines might be for an alarm service, which dials out to notify the repair service of an out-of-tolerance condition, or for checking on the quantity stored in a hydrogen-filled tank.

OTHER VITAL EQUIPMENT LOCATED IN THE PBX ROOM

Other important equipment is typically located in the same room as your PBX. After the critical devices are identified, make sure they are protected and draft a plan to fully recover them. These devices may include:

- ***Interactive Voice Response (IVR).*** Gives callers information based on what the caller enters using the telephone keypad. You have heard the messages—please select 1 to talk to sales, select 2 to talk to. . . . These audio tracks should be backed up and the queuing logic documented.

- ***Intelligent Port Selector.*** Connects the incoming call to the first available line. This is used when you have multiple people answering inbound calls, as in a hotel chain's reservation center.

- ***Call Management System.*** Monitors the volume of telephone calls during peak periods, to identify the number of telephone operators needed and to track operator efficiency.

- **Call Monitoring.** Tracks the level of call activity by showing the status of the trunk lines, the number of calls in progress, the number of calls waiting in queues, the wait time, the number of abandoned calls, and the status of the operators.

THE TELEPHONE COMPANY'S CENTRAL OFFICE

Soon after telephone service was first created, it became obvious that every person could not be wired to every other person they might possibly want to call. This would result in an impossible maze of wires. To call someone new, you would first need to run a wire from your telephone to their telephone. Imagine the problems in asking a girl for her telephone number in those days!

To simplify this problem, all the telephone lines were run from the customer into a central building. There the switchboard operators would physically patch your telephone line into the switchboard, making the connection. These buildings would be located at various places around the city and were the central places where connections were made. Eventually, automated switching made it easier, but buildings were still needed to house the automatic switching equipment. In more recent years with the advent of solid-state circuits, the floor space required for these buildings has shrunk dramatically. You still see them around: small buildings without any windows, usually neatly trimmed grass, and a small telephone company sign by the front door.

The central office provides a similar service to a PBX by switching your call to another local telephone, to a different central office far away, or to a long-distance carrier's point of presence (POP). The long-distance company then routes the call through its switching center and back to a distant central office and down to the faraway telephone.

INTEREXCHANGE CARRIER POINT OF PRESENCE

With the breakup of the AT&T long-distance monopoly in 1982 came the creation of independent long-distance telecommunications providers. These non-AT&T long-distance providers are known as Interexchange Carriers (IXCs). Along with this choice came the opportunity to split the company's long-distance service across different carriers in hopes that all of them would not be knocked out in the same disaster and therefore your communications traffic could still flow out on the alternative pipeline. For that to be true, a lot of careful planning is necessary.

First, you must ensure cable routing separation so that you have a different wire path from your facility to the IXC's point of presence. Most companies are a mix of owning the network in high-traffic areas and leasing capacity from another carrier in a low-traffic area. This means your physical traffic separation may only be on paper. If you are in a high-traffic area, the carrier may run a separate cable to your facility. If you are not, then you will probably connect to the IXC in the nearest central office. Ask your carriers if they share lines with another company. Also, request to see the physical route of the cable.

Some telecommunications experts believe that route separation is much more important than using multiple telecommunications companies. They feel it is easier to manage one supplier as long as the cable routing issue is addressed. When choosing an IXC, things to consider include:

- What is their system availability time, and what will they guarantee?
- What are the consequences to the IXC of downtime? You can ill afford it. A few extra free minutes of service every month is poor recompense for missed customer calls.
- What is the restoration priority for the sections of the network that you will be using?
- What are their alternate routes for the places you typically communicate with? Don't automatically assume a new carrier will be a better alternative to your existing carrier. Is your service route a spur (single-threaded) service? Is it a ring architecture, which at least gives you two paths in case one has a problem?
- How often does the carrier practice its disaster recovery procedures?
- How easily can the IXC shift your inbound calls to another site?

Okay, well, this all sounds straightforward. After all, telephone service has been around for well over 100 years and its technology is well known. *What could possibly go wrong?*

Older telephone systems use an analog technology that cannot share the same wire as digital communications. Plans for recovering these systems include a backup PBX and all of the support equipment.

DIGITAL TELEPHONE NETWORK

Running two separate circuits to each desk (an analog line for telephone and a digital wire for data) is expensive. As more devices became "smart" (they are really special-purpose PCs running logic), the switch to using the data network for everything was easy. Today, fax machines, telephones, and all other communications devices use the digital communications network. This makes writing a telecommunications recovery plan much easier as a single line per workstation is all that is required.

Most companies have converted from analog telephone systems to Voice-over-Internet Protocol. VoIP sends your telephone traffic through the workstation's data connection and then on through the Internet. This avoids wiring a second network. The VoIP telephone converts the audio of your voice to a digital signal and then handles it like any other IP packet. This packet is then routed to its destination. However, each packet is not acknowledged as an email would be. A dropped packet is simply not received and most conversations skip over it. A VoIP network uses:

- ***A VoIP telephone instrument***—a handset or telephone dialing pad—which

- ***Wiring***—VoIP uses the existing data network wiring, switches, and routers.
- ***A server***—Required to manage the VoIP communications, this device runs software for switching traffic to the right connection at the far end. The server usually sits in the computer room, so the environmental controls and security are already in place. Redundancy for the VoIP server is necessary because, if it stops, then so does the company's telephone service. (For this reason there are usually several traditional telephone circuits in the security office.)

One reason digital phone runs so well is that the telephone company uses this technology with your calls once it leaves your building anyway. VoIP brings these savings:

- Eliminates the expense of running the analog cable and all its support equipment.
- Eliminates the cost of a second cable for cabling moves.
- Saves the cost of a PBX and its associated equipment (but adds in the cost of a server to route the traffic). Often the PBX sits in its own environmentally controlled room whereas the server is in the data center.
- Eliminates long-distance calling charges.

Softphones are an attractive idea for initial recovery from an office disaster. By running the telephone connection through the PC there is one less thing to recover. The challenge comes from the PC itself. Since the device is usually running other software at the same time, we have all experienced a PC suddenly slowing down while something runs in the background. When this occurs in the middle of a call, the conversation may seem to have ended.

COMPUTER NETWORK BASICS

All but the smallest firms today have one or more data communications networks within their organization. A network consists of one or more servers that are connected to one or more workstations and allows users to share information and resources. This connection can be by copper wire, fiber-optic cable, or even radio frequency (RF), which is wireless. Rarely are workstations connected directly into a server. Typically, they plug into a wall jack, which is connected to a wiring closet. In the closet will be one or more network-switching devices that will connect the local devices to a router in the computer room. The wiring closet is often the same room that receives the telephone wiring.

In the computer room (either a central location or possibly rooms sprinkled about the facility) sit the servers. A server is a computer that runs software to provide access to resources attached to the network, such as printers, disk storage, and network applications. A server can be any type of computer that supports the sharing of resources. A server may be a standard desktop PC or a dedicated device containing large amounts of memory and multiple storage devices that can support hundreds of devices at the same time.

The network begins at an end-point device that communicates with other devices. Typically, this is a desktop workstation but could also be a printer, a data collection device, a cell phone, or other device for collecting or displaying data. Networks are generally described by the scope of their connections (local or wide area).

PERSONAL AREA NETWORK (PAN)

The smallest network is called a Personal Area Network (PAN). It may also be referred to as a piconet. A PAN is often centered on a cellular telephone or tablet PC. It uses Bluetooth technology to communicate with nearby devices. Bluetooth has a maximum rated distance of 30 feet, but that depends on the strength of the signal and the electrical properties of any obstacles between the transmitter and receiver.

Examples of PAN devices include:

- Electronic watches that display messages from the cell phone
- A car's cellular telephone hands-free connection
- A wireless router to use wireless data instead of cellular minutes
- Internet-connected home appliances that also interact with your cell phone

The challenge of a PAN is if some of the connections are to the company's business equipment. For example, a cell phone is compromised by a malicious person who uses it (as a trusted source) to connect with the company's wireless router. "Smart" cell phones contain powerful processors and a lot of memory. They can often connect to company applications and, in some cases, update files. This makes smartphones a valuable tool for accessing centrally stored recovery plans in an emergency since just about everyone has one.

The most basic type of network connection is a modem and an analog telephone line. This is the slowest and most unreliable type of connection, supporting up to 56 kilobits per second (kbps). Although dialup communications are becoming rare, they still exist for special-purpose applications.

LOCAL AREA NETWORK (LAN)

A LAN connection starts with each piece of equipment on the network being connected by wire to the wall jack, which is in turn connected to a wiring closet. A wiring closet for your computer network is usually located near a group of workstations. Typically, there is one for each floor of an office building. The wiring closet consists of many different cables running in spaghetti-like fashion to a network switch. The devices attached to a switch make up a LAN.

The network switch provides some traffic isolation between devices. This circuit isolation improves the network's overall performance by keeping the traffic unnecessary traffic. The devices attached to the switch communicate based on their IP (Internet Protocol) numeric address.

When someone on a LAN needs to communicate with a different LAN, such as when a user wants to access their email system, then the traffic is passed on to a router. A router connects LANs and provides further network isolation. Connecting LANs together makes a WAN. Router software may also provide a layer of information security through a series of business rules about what traffic is permitted to pass and which users may perform certain actions.

When writing a recovery plan, ensure there is up-to-date documentation of which people are connected on what LAN and any business rules in the routers. Both the connections for individuals and the business rules change over time.

WIRELESS NETWORK

A wireless network is like a wired LAN except it uses radio frequency waves to communicate with portable devices. The range and data throughput depends on the technology used. Instead of network switches, wireless networks use Wireless Access Points (WAPs). These access points connect to the end-point devices (PCs, cell phones, scanners, special tooling, etc.). Security is provided through encryption that can be enabled on the devices. Recovering a wireless network requires a list of the devices, protocols used, and WAP locations.

A wireless network is based on a site survey. This survey examines the impact of the facility's structure and furnishings on the radio frequency traffic to identify coverage areas without coverage (dead spots). The survey indicates the optimal placement of wireless access points for the desired coverage. The desired signal strength and avoidance of coverage outside of the building will determine the types and placement of antennas. Wireless coverage areas should overlap between 10 to 15 percent to enable device roaming. Too much overlap may cause interference.

Each wireless access point will require a wired network connection and electrical service. They also tend to be installed high up in the ceiling or on walls, requiring some sort of mounting bracket. An adjustable mounting bracket enables easy repointing of antennas.

WIDE AREA NETWORK (WAN)

A Wide Area Network connects LANs. This can be within the same facility, between facilities, or across the country. There are other names for WANs but essentially they connect LANs. WANs are concerned with the type of connection and the secure passing of data.

WANs can connect two ways:

1. Dedicated data line used between company data centers. A dedicated line is expensive but provides control over who can connect to it. A dedicated line is engineered from end to end and takes weeks to obtain.
2. Shared data line. This is the common approach to connecting data centers. A shared data line sends traffic through the Internet via high-speed connections. A Virtual Private Network (VPN) uses encryption to provide a secure connection through the public Internet. VPNs are also commonly used to encrypt traffic for people who work from home.

INTERNET SERVICE PROVIDERS (ISPS)

ISPs connect your organization to the Internet through one of the network connection options listed previously. Most organizations will have only one physical connection between their network and the ISP for Internet access. If Internet access is critical to the operation of your business, you should consider a connection to a second ISP to give you a second pathway to the Internet. There are, however, several things to evaluate and plan for when considering a redundant ISP. (This is similar to considering multiple telecommunications companies.)

Ensure cable separation so that you have a different wire path from your facility to the ISP's point of presence. Most ISPs are a mix of owning the network in high-traffic areas and renting from another ISP in a low-traffic area. This means your traffic separation may only be on paper. If you are in a high-traffic area, the ISP may run a dedicated high-capacity cable to your facility. If you are not, then you will probably connect to the ISP's nearest point of presence. Do not take for granted that because you use two ISPs you are on two different wires. Ask them if they share lines and ask to see the route of the cable.

Some telecommunications experts believe that route separation is much more important than using multiple ISPs. They feel it is easier to manage one ISP as long as the cable issue is addressed. When choosing an ISP, things to consider include:

- What is their system availability time, and what will they guarantee?
- What are the consequences to the ISP of downtime? You can ill afford it. A few extra free minutes of service every month is poor recompense for missed sales due to the Internet being unavailable.
- What is the restoration priority for the sections of the network that you will be using?
- What are the ISP's alternate routes for the places you communicate with?
- How often does the ISP practice its disaster recovery procedures?

RISK ASSESSMENT

When developing your telecommunication services disaster recovery plan, look for single points of failure that will adversely impact your critical business processes. These critical processes should have been identified in the Business Impact Analysis. External threats to telecommunications include cables being cut, interference from electromagnetic sources, attacks by hackers and other water pipes can damage cables and equipment. In an ideal world, you would have duplicate service running to each telephone or desktop.

Externally, an issue with multiple Internet connections is that there are now two points of potential entry for hackers. Internally, it is usually not cost-effective to run duplicate cables. An alternative is to install an extra jack for every few cable drops. If a problem occurs in an end-user's cable, the extra jack would be available as a backup until the problem cable is repaired.

It is also important to review vulnerabilities to problems with the devices that connect the telecommunications network together, such as routers, switches, and firewalls. Your Business Impact Analysis should determine the impact to the company if one of those devices should fail. Consider installing redundant devices with fail-over software that can take over if the primary device fails.

Wireless telecommunication connections can provide an effective backup strategy if the wired network fails. Wireless networks have no wires to fail and can be quickly installed if needed after a failure in the wired system. (Of course, the wireless access points are themselves connected to the network using wires.) The major drawback to using a wireless network is that the transmissions can be intercepted. Use encryption and other security measures to prevent others from intercepting your network traffic.

Consider using network monitoring software that can detect problems on the network. Network monitoring software can alert you immediately if a node on the network is having problems or has failed, which will allow you to restore service more quickly and help prevent problems from cascading. Most network monitoring software can be configured to look for system parameters that fall out of the desired range, indicating a device that is beginning to fail. It then generates a message to a support person to act.

NATURAL HAZARDS

Now that you know the basics of how your telecommunications systems work, what are the risks to these systems? Chapter 3 discussed natural hazards in detail, so this section only addresses those natural hazards that have a major impact on your telecommunications systems.

- ***Ice Storms and Blizzards.*** Ice can coat cables strung from telephone poles and, if the weight is great enough, potentially bring them down.

- ***Thunderstorms and Lightning.*** Severe rain can weaken the ground around a pole and cause it to sag when there are high winds at the same time pushing against it. Lightning can strike telephone poles and send a major charge flying down the line, burning up wire and your equipment along its path. Also, falling trees can bring down cables strung along telephone poles.

- ***Tornadoes.*** This powerful destructive force can snap lines and rip up telephone poles. High-risk areas are prime candidates for buried lines.

- ***Hurricanes and Floods.*** They can cover a wide swath of land and not only bring down a telecommunications network but also prevent crews from promptly addressing the problems.

HUMAN-CREATED HAZARDS

People are just as big a danger to your telecommunications systems as nature can be. Human-created dangers include:

- ***Breaks in Buried Lines.*** Sometimes emergency excavation is necessary (such as repairing a broken gas main). Sometimes the local government is cleaning trash out of the ditches alongside the road. Sometimes a well-meaning person just digs without asking (including on your own property). In any of these cases, there is the chance that your tiny little cable will be dug up and severed.

- ***Accidents.*** Sometimes drivers miss the tight turn and break off a telephone pole. If this is your only line to the central office or your ISP, your service is gone until the pole is replaced.

- ***Central Office or ISP Failure.*** A problem in a central office or with your ISP can quickly shut down your telecommunications unless you are wired to a second provider.

Networks are a long chain of devices working together. A chain is only as strong or resilient as its weakest link.

TELECOMMUNICATIONS AND NETWORK EQUIPMENT ROOM

The room that houses your telecommunications and network equipment may not be as safe as you think it is. Dangers to your telecommunications room include:

- Temperatures that are too hot, too cold, and that swing widely are all hard on your telephone switching equipment. Extreme temperatures stress the printed circuits. Large swings in temperature (hot to cold) cause expansion and shrinkage of circuit cards and again can weaken components over time.

- Humidity magnifies temperature and enables the growth of mold on your equipment.

- Loss of electrical power will stop a PBX, routers, switches, and other telecommunications equipment from working. Cell phones and direct lines out should still be operational since these telephone circuits supply their own power.

- Water pipes overhead in your telecommunications room could release water onto sensitive equipment. The same goes for the cable panels. Overhead pipes along external walls could potentially freeze and leak when thawing. Leaks from rooftop air-conditioning compressors are also a problem.

- Physical security may be a factor. This room is not set up to accommodate tourists and they should not be allowed in. Always keep the door locked.

- Fire is a possible danger. This equipment generates heat and is in danger from

CABLING

The discussions earlier about wiring closets had a purpose. Imagine the mess if an isolated fire in the wiring closet melted all these wires. In terms of structural damage, you got off easy. But in terms of damage to the telecommunications system, that entire area of the facility will be without service for some time. New cables must be run from the PBX or network switch to the closet and from the wall to the closet. The alternative is to splice an extension onto each cable and run it into a punch block. Either way it is time-consuming and expensive. It is a good idea to keep everyone out of the network closet and to never store anything in the closet that might cause a problem.

INTERNAL CABLING

For disaster avoidance, concerns begin with the wiring closet and patch panels. Take a walk with your telecommunications specialist and identify the location of all telecommunication patch panels in your facility. Things you are looking for:

1. In a closet

a. The door and any windows are kept locked.

b. There is fire suppression equipment (usually fused link sprinklers).

c. There is nothing else in the closet except telecommunication and/or data communications equipment. Combustible materials stored in the closet threaten the sensitive equipment. This is not the place to store holiday decorations, old files, office supplies, or janitor supplies.

d. Very few people have keys—telecommunication support staff, security, and no one else.

e. There should be sufficient light to work in the closet.

f. There will often be data network wiring and telephone switching equipment together in these closets. They are a natural fit here. The network equipment is energized electronics, which will generate heat and introduce a potential fire source.

g. Be sure there is good air circulation so the heat created by the equipment has an outlet. This is usually through vents cut in the door at the top to let heat out and at the bottom to let the cool air in.

2. Outside a closet

a. Be sure it is covered and the cover is locked. Same rules for the keys as for the wiring closets. Enough keys for the right people and none for anyone else.

b. All cables and wires leading into the external panel are encased in heavy conduit to inhibit tampering.

c. If the patch panel is in a warehouse or factory, be sure it is strongly protected from environmental influences (e.g., leaky ceilings, dust) and from being crushed by a forklift or toppling stacked material.

EXTERNAL CABLING

The first rule of outside cabling is "cabling and backhoes don't mix!" A chain is only as strong as its weakest link. Your servers and PBX are snugly locked up in their room, and the ISP's office and the telephone company's central office are also secure. However, the wire in between is exposed to the ravages of weather, people, and machines.

External cabling runs from your building to an access point along the road, usually on a pole. Then the wire runs through the countryside (usually along a road or railroad) to a point of presence or central office. In the city, it might run through underground pipes to the point of presence or central office. You have no control over where the wire is run and no capability to protect it! In some areas, you will even have separate cable runs to be concerned about—one for the local telephone company and another for your Internet service.

A common term used when describing part of a telecommunications network is "the last mile." The last mile describes the wire from the telephone company's central office or the ISP's point of presence to your structure (and it is usually more than a mile). This is also known as the "local loop." This part of the network is the most vulnerable.

ROUTE SEPARATION

The best path to telecommunications reliability is redundancy. This can include redundant equipment, redundant technicians, and redundant cabling. The more alternate paths that a signal can be routed, the more likely it is to get through. The principle of cable route separation should be an integral part of your telecommunications network design. Essentially this means that you have more than one cable between your building and your telecommunications providers. This prevents a total communications outage from a single cable cut.

Few companies can afford to take this to the extreme, but you can consider these steps. Begin by asking the telecommunications provider to show you the physical route that your cable takes from the wall of your building to their office. This will also show you how exposed the cable is to auto accidents (are the poles close to the road?), to backhoes (is the cable buried along the road in some places?), or any other number of threats.

With this experience in mind, negotiate with the telecommunications provider a fresh cable run from your building (exit from the opposite end from the other cable) to a different central office or point of presence. This will keep you operational in case your usual point of presence is damaged or experiences an equipment failure, or if the cable to the point of presence is broken. How likely is that to happen?

In May 1988, there was a fire in the Illinois Bell central office located in Hinsdale, Illinois. The two-story building was completely gutted. This building was an important hub for Illinois Bell, as well as for major long-distance carriers. In addition to cellular service and data networks, approximately 40,000 subscriber lines and six fiberoptic

To reduce the chance of a total system failure like the Hinsdale disaster, the telephone companies have gradually migrated their central office structure from a spoke-and-hub approach (with its obvious single point of failure) to a ring or mesh approach, in which multiple central offices are connected to each other. In this scenario, calls are routed around the damaged central office in a manner that is transparent to the caller. This is gradually being implemented in rural areas and small towns. If possible, you want routing separation with the wires running from your facility running to two different central offices on separate routes.

Route separation is more important than having multiple vendors. Most cable routes follow railroad rights-of-way and the major carriers' lines commonly converge at bridges. Imagine the number of places there are to cross a major river or highway. There aren't many to choose from. The lines from various companies often come together here and cross under the same portion of the bridge. What could go wrong? Vehicles crossing bridges might catch on fire, river barges can break free and strike bridge pilings, and major bridges are tempting terrorist targets.

Many telecommunication providers define cable separation as a distance of 25 feet or more between cables. Others ensure cables are at least 100 feet apart and have at least a two-foot separation at cable crossovers. Ask your Internet, local, and long-distance telephone carriers how they define cable route separation and how faithful they are to that standard. When using multiple vendors, even if their cables are separated, they share a common weakness if they join at the same point of presence or cross a river under the same bridge. Upon close investigation, you may even see that where you are using two companies, one is leasing part of the same wire from your other provider!

MAP IT OUT

Now that you know the cable route to the telecommunications provider, map it out—from where it enters your wall to the provider's point of presence. You might think, "Isn't that the telecom provider's responsibility?" The answer is "yes," but you need to know the level of risk the company is carrying. If you drive to work using the same route as your cable, you might see construction crews digging near where the cable is to repair a water main, snapped poles, or sagging wire due to accidents or severe weather—any number of threats too close to the wire for comfort.

So, draw out a map of where your wire runs from the telephone pole outside to the telecommunications provider's office. Then make a detailed map of the run from the pole to the wall and on to the wiring closet room. Indicate which lines terminate in equipment provided by the telecommunications provider and which lines provide essential services.

DEVELOPING A PLAN

This section describe issues to consider as you develop a disaster recovery plan for your telecommunications assets.

WHAT ARE WE PROTECTING?

As you know, the first step in building a plan is to make an inventory of your telecommunications assets. You will assemble at least four lists. The first lists every major item and who to call if it breaks. The second shows the location of the main cable runs in the building. The third is a map of your wireless coverage within the facility. The fourth includes all the telephone numbers used by the facility. In a crisis, you may need to reroute some of these to another location.

1. Begin with a list of all major devices in your telephone switching room and network room, such as the PBX, IVR, network switch, and data router. Include on this list:

a. A description of each device.

b. The serial numbers of the main equipment and any major components.

c. The name, 24-hour telephone number, contract number, and contract restrictions for whoever you have arranged to service that item.

d. The location of every item, including a simple floor map of all telecommunication rooms.

e. Backup details. Be sure to back up your entire configuration data, either on magnetic media, cloud storage site, or if the file is small, print it and store it safely away.

2. Now make a wiring inventory of all the cable runs within your facility. You do not need to show individual runs to the offices. In a crisis, you can always shift someone to another office. The wiring inventory is best accomplished with computer-aided drafting software on a digitized version of the floor plan.

a. Indicate the runs on maps of each building or floor of a multistory building. Knowing the location of these cable runs is important to quickly assess damage.

b. Indicate where the telecom service enters the building and its route to the telephone exchange and network rooms. Note any hazards along the cable path.

c. Record contact information for whoever is supporting your cabling.

d. If you have any independent direct lines that bypass your telephone switch, mark them on the map.

3. Using the site survey, create a wireless coverage map.

a. Identify the location of every wireless access point and its communications and security configuration.

b. Document the business purpose of each connecting device and its configuration.

4. Make up a telephone number inventory with all the telephone numbers assigned to your building/facility, including:

a. DID (Direct Inward Dialing) lines.

DETERMINE THE TELEPHONE CIRCUITS' RESTORATION PRIORITY

Telephones are used to communicate, and every part of the company uses them differently. In an emergency, salespeople will need to contact customers, the warehouse will need to call suppliers, and the people at the disaster site will want to call home. In a disaster, you won't be able to please everyone right away, so you need a restoration priority guideline to know which circuits to recover (or protect) and in what order.

Start this analysis by reviewing the critical functions identified by the Business Impact Analysis. Next, meet with representatives from each department and ask them to identify their critical telecommunications needs and at what point in the disaster containment/recovery they would be needed. For example, early in the emergency, the Human Resources team might need to notify employees to not report to work or to come in at certain times. Each department must prioritize its communications needs.

With your critical communications functions identified, you can determine which circuits support these key functions. If you trace out the top three or four circuits, you may see some of the same hardware, some of the same cables, and the circuit paths common to them all. Working down your list, you can see which of your hardware devices (or cable bundles) has the greatest benefit to being restored first.

You must also include in your plan how you will relocate operations to another site. This is a twofold issue. In the first case, if a department must be moved off-site due to damage to its offices, you need to be able to shift its inbound calls to the new location quickly. In the second case, if your telephone equipment room is destroyed, you must quickly restore a minimal level of service. Some people might plan to build a new telephone room onsite. Others will contract with a service company that will bring a telephone equipment room to your site already set up in a large trailer. The recovery company needs to plug into your wiring (no trivial task). This could buy you time until your equipment room is rebuilt. If you elect to bring in the configured trailer, this agreement must be made in advance; be aware, however, that these options might not be available in a wide-area disaster.

REVIEW NETWORK SECURITY

Your network has some unique security issues to consider. The first is physical security. No one except the network support staff should be allowed in the network closets. The network administrator must work with the facility's security manager to ensure that these doors are always locked. Depending on the airflow in the closet, some vents may be added to the doors.

Sometimes network equipment is in freestanding cabinets instead of closets. These cabinets must be locked just like the closets and the keys held by only a few people. In a large facility, this can add up to a lot of keys. Your goal is to minimize the number of keys by using a sub master key for all closets and, if possible, a sub master key to all cabinets. These keys must be tracked and, if lost, a determination made whether to rekey the locks.

The next area to consider is logical security. The network software on the servers and in the network devices will be, in some cases, password protected. These passwords should be protected like any other and known only to the key network support staff. However, they should also be written down and locked in the Data Processing Manager's office in case the network staff is unavailable. (In a wide-area emergency, the network manager or key staff members may not be available or able to come in.)

Include a clause in your Acceptable Use policy that no one is permitted to plug privately owned devices into the network. This is to stop people from plugging in their home notebook PCs and bringing down your network. In addition, contract employees should never be permitted to connect their equipment into your network. The same policy should cover connecting to your wireless nodes.

Because servers can support many users and are used to host critical applications, loss of a server can have a severe impact on the business. Certain processes can ease the restoration of servers. For example:

- ***Store backup tapes and software off-site.*** Follow the procedures discussed in Chapter 4 for handling and storing backups. Backups of data and application installation media should be stored off-site in a secure, environmentally controlled facility.

- ***Standardize hardware, software, and peripherals.*** Standard configurations of these items will make restoration much easier. The standard configurations for hardware, software, and peripherals should be documented in your plan.

- ***Document the network.*** The physical and logical network diagram must be kept up to date. The physical documentation should include a diagram of the physical facility and where the primary cables are routed. The logical diagram shows the network nodes and how they interconnect. Both diagrams are critical in restoring the network after a disaster.

- ***Document vendor information.*** Maintaining up-to-date information on the vendors you use for hardware, software, and peripherals will make it easier to restore your operations.

- ***Work with your security team.*** The more secure your systems are, the less likely you are to have a data loss due to a security breach. You'll also want to be sure you can restore the latest level of security if you must configure new servers after an emergency.

TELECOMMUNICATIONS MITIGATION PLAN

With these risks in mind, along with due consideration of the identified priority circuits and equipment, you can assemble a mitigation plan to reduce the likelihood of a threat or its impact if it occurs. The key to telecommunications mitigation is redundancy. Redundancy in equipment is important in case one machine must be repaired. Redundancy in communications routes is important in case a cable is severed or interrupted. Redundancy in communication methods, such as radios, cellular telephones, or satellite communications, will provide at

Your cable mitigation plan should consider the following:

- ***Multiple paths for the "last mile."*** Investigate the path from your telecommunications equipment room all the way to the central office or point of presence. Ask the telecommunications provider to make another connection from your PBX or Internet server out through the wall of your building at a point distant from the other exit point and on a different route to a different point of presence. Be sure your in-house wiring staff understands what you are asking for before they start.

- ***Multiple paths for IXCs.*** Investigate the path from your telephone equipment room to your service provider's point of presence. Avoid the same route as used for your local telephone service.

- ***From the pole to your wall,*** if the cable is underground, ensure it is clearly marked with "do not dig" indicators or other obstacles to keep digging equipment away (or at least delay them until the cable can be marked).

TELECOMMUNICATIONS EQUIPMENT ROOM MITIGATION PLAN

Think of your telecommunications room like a computer room. Their environmental and security needs are almost identical.

- ***Uninterruptible Power Supply (UPS)***. When you lose electrical power, this is what will keep your PBX or Internet server active until external power is restored or until your facility's electrical generators kick in. Conduct a power loss test to verify which equipment is and is not connected to the UPS. If the device isn't essential or time-consuming to restart, take it off the UPS. The fewer machines draining the UPS batteries in an emergency, the better. When conducting the power test, see how long the batteries can support the load. Be sure the UPS is properly maintained by your service company.

When Hurricane Hugo struck the Southeast United States in 1989, it surged hundreds of miles inland with huge amounts of rain and wind. The storm downed so many trees that it was days before electrical power was restored to some areas. Even the emergency batteries at the central offices were eventually drained. So, do not depend solely on your UPS for emergency power. Consider other power sources as well.

- ***Fire.*** The telecommunications equipment room requires the same fire protection as a computer room. An early-warning fire alarm system and gas fire suppression system are highly recommended.

- ***Security Access.*** This room is usually unattended. It should be locked as no one has any business strolling around in this room. The telecommunications system administrator can perform most administration duties via terminal over the network.

- ***Structural Investigation.*** Although you can rarely select the room, a close inspection can identify problems. Water pipes running along the walls or along the ceiling are a potential source of problems. They may freeze or leak. They should be watched carefully. Consider installing a plastic shield attached to a drain placed under them to catch condensation or leaks. A roof-mounted air-conditioner may cause a roof leak. External walls may stress the air-handling equipment as outside temperatures heat or cool the walls.

- ***Temperature Variability.*** Your equipment must be in an area that maintains a specific operating temperature and humidity range for maximum life. This is also essential to maintaining your service agreement coverage. Proper air-conditioning, heating, and humidity control equipment must be well maintained.

- ***Alarms for Humidity, Temperature, Fire, and Electric.*** A bank of alarms will help you monitor the condition of the room. These alarms must sound within the room, as well as at the security guard station as the room is normally unattended. Early detection will reduce the likelihood of significant damage. Include automatic paging equipment for notifying the after-hours support team of problems. Consider installing automatic shutdown software for your equipment, which signals your hardware to shut itself down gracefully in the event of a problem.

- ***Data Backups.*** Like a computer, your switch and configurable devices need to back up their configuration data whenever there are changes. Store copies of these files in a secure off-site location or in cloud storage.

ALTERNATE COMMUNICATIONS METHODS

You must have written procedures for quickly routing IXC traffic to the local telephone service in case your IXCs have major problems. How hard is this to do, and then to switch it back again? Is it easier (or cheaper) to split the load across two carriers and then shift the entire load to the functional carrier? Other items to consider:

- Do you have company-owned cell phones that can be used for communicating when the telephone system is inoperable?

- Are there written procedures for how to work with the telephone company to shift specific telephone numbers or all incoming calls to a different company site?

- Do you have any employees who are ham radio operators? It is nice to have alternative channels when the primary ones are not available. In a wide-area emergency, radio communications will also get congested. Radio conversations are not secure and anyone with the proper equipment can listen to them. Radio communication is also slow and not suitable for large data volumes.

- If you have other communications alternatives such as satellite and microwave, have you considered that both are susceptible to problems if the antenna has been shifted by a storm or earthquake?

ACTION STEPS FOR YOUR PLAN

Most companies contract emergency recovery of their telecommunications room is destroyed and to set up a trailer adjacent to your building with a ready-to-go telephone switch and Internet connection. To support this, companies often run cables to the front of the building for a quick connection.

Cellular telephone traffic can be somewhat limited in a wide-area emergency as the local cell towers become saturated with calls. Use the cell phone network as an alternative communications channel, not as the primary backup.

A branch office is an ideal place to shift operations to until the disaster-struck site is recovered. The key is how far away the backup facility is located from the affected site. It should be far enough away to be unaffected by the same disaster. There is no set mileage distance but it should at least be on a different power grid and telephone central office. If it is too far, then you must also provide lodging for the relocated people.

One problem is how to relocate to these sites in a crisis. If this is during an area-wide disaster, mass transit such as air travel may be disrupted and driving there yourself may be difficult. One side aspect of the attack on the World Trade Center in September 2001 was that it shut down all air travel. Companies scrambling to activate their out-of-state recovery sites had a difficult time shifting key personnel and material to the site. No one had planned for a complete shutdown of the air transportation system.

Things to consider after a disaster:

- Do not make any unnecessary calls—only for emergencies.
- When calling, you may need to wait several minutes to get a dial tone. Do not hit the switch hook, because every time you do, you are placed at the end of the line for the next available dial tone.
- When you receive a dial tone, quickly dial your number. In a time of low telephone service availability, the dial tone is offered for a much shorter time.

CONCLUSION

Modern businesses rely on their data networks and telecommunications to function in the marketplace. As with any other important business resource, we need to be familiar with the network's role within our operation and how its absence will affect us. Redundancy is your best defense against a disaster removing your ability to communicate with customers and suppliers. A thorough understanding of your organization's telecommunications requirements will help you to design the most cost-effective plan to protect your connection to the world.