IM**IA WGP 23 (02) E**

Telecommunications and e-Commerce - Global Exposures

Presented at the IMIA Conference in September 2002 by
Michael Petruzzello of Hartford Steam Boiler, Hartford.

Telecommunications and e-Commerce - Global Exposures

Introduction

Despite the global economic downturn in the telecommunications industry, telecommunications equipment technology continues to rapidly expand. This paper examines equipment breakdown risks associated with switching and transmission equipment that compose a telecom network. Part 1 focuses on the telecommunications industry itself, from service providers to the end users. Part 2 takes a look at the impact of telecom equipment has on the e-business industry.

Part 1 – The Telecom Industry

The telecommunications industry is not only characterized by technology, but also by acronyms and definitions that originated in governmental enactments intended to regulate telecommunications service companies. For the purposes of this paper, discussion will be limited to the technical realities. Acronyms and jargon will be used only when necessary.

Telecommunications is Complex

Telecommunications equipment has evolved from a simple device that conveyed voice over modest distances (telephony) to complex media that transfer voice and data worldwide. Telecom now uses analog and digital technology, and fiber-optical conductors.

The development of cellular telephones illustrates the complexity of telecommunications today. A small radio transceiver — a cell phone — is continuously tracked by a system of cell towers. When we place a call to the office, the transceiver contacts the nearest cell on one of hundreds of available frequencies. Using full duplex transmission, it connects our call through the cellular switching network to the local telephone network in the vicinity of the office. The call is ultimately connected to the line and telephone that corresponds to the number that was dialed.

These events occur in about five seconds. The availability of this service is so robust that we become annoyed when we encounter perfectly understandable limitations imposed by terrain or cell-tower density.

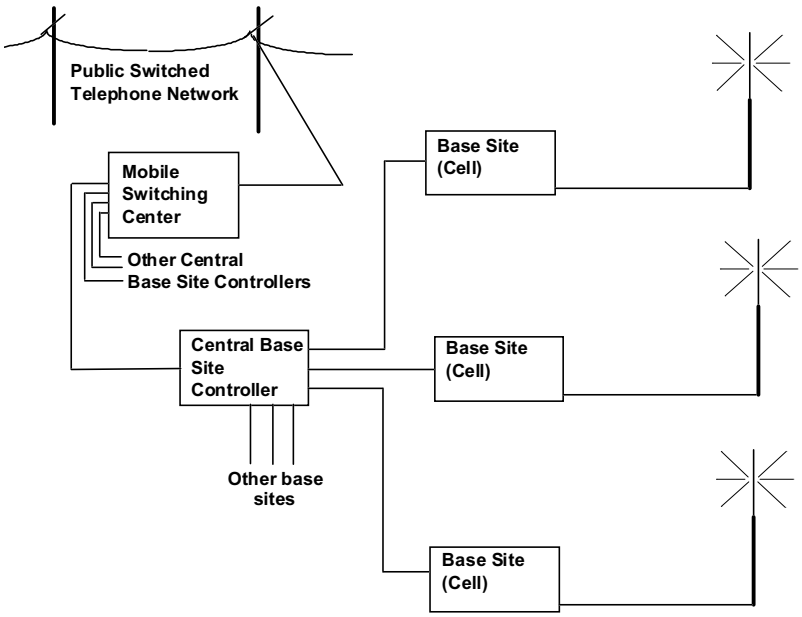


Figure 1

Figure 1 shows only the portion of the cellular telephone system that connects the cell antenna to the public switched telephone system. A more complex network makes the connection to the dialed telephone number.

The Technologies of Telecommunications

Virtually no electronic or digital technology is *not* used to manage telecommunications. Although the majority of telephone sets are still connected to copper wire (analog), the network handling the calls uses digital computers, a variety of multiplexers, solid-state and analog switches and satellite, radio, and microwave links. Recently, telephone connection using the same broadband cable that provides television and Internet service has become a reality. This development may indicate that broadband cable is destined to be the telephone connection of the future. Copper telephone wire can be displaced with fiber-optic cable.

The essence of a telephone network is its ability to switch connections. Originally, telephone circuits were actual electrical circuits, switched at the local telephone office by human operators who used a switchboard of patch cables and plugs. That same function survives, but a computer system using solid-state electronics serves as the physical switch.

Another aspect of the network is the successive concentration of connections from the individual telephone set toward the center of the network.

Figure 2, below, illustrates this principle. Individual telephone lines are connected by local telephone wiring to a central office (sometimes called an exchange), where they are then connected to terminals on the central office switch (sometimes called a signal switching point, or SSP as shown here). The central office switch can then connect the individual telephone line to one of several trunks (sets of wiring or fiber optic lines) that connect the central office switch to other switches in the network.

Eventually, a connection can be made through a succession of switches to another telephone line in another geographic location. However, all connections are redundant from the point where the individual telephone line connects to the central office switch to the corresponding point at the remote telephone line. Figure 2 shows that there are at least three separate routes available to make the connection.

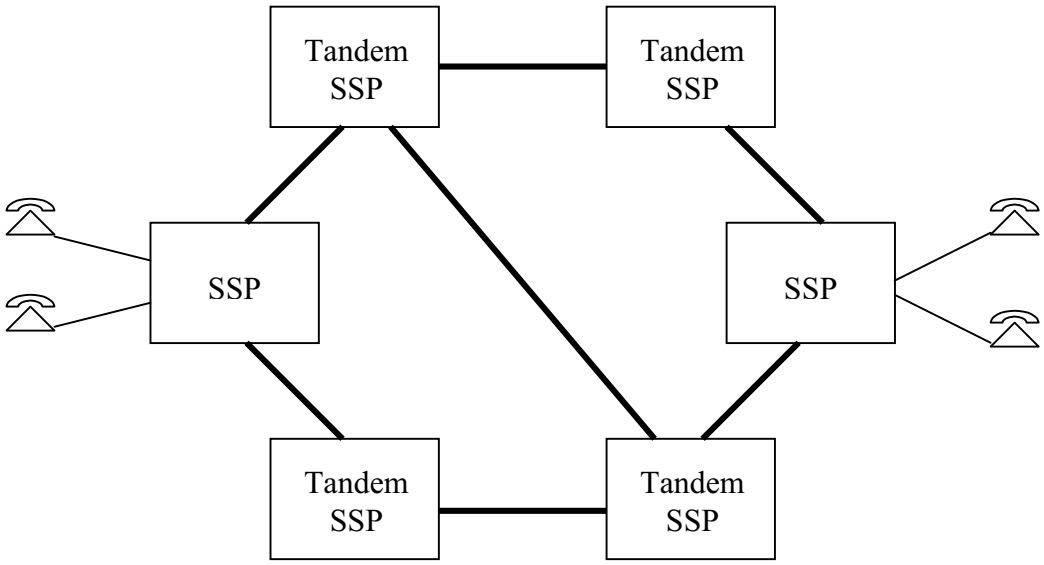


Figure 2

Note here that the lines connecting the SSPs in this diagram will be referred to as trunk lines, or trunks, in this discussion.

Figure 2 illustrates how telephone systems work. It is not significantly changed from the days of human operators except switching and trunk design have advanced. Connections between telephone offices can now involve microwave links, fiber-optic links and sometimes satellite links, in addition to traditional copper conductors. Switches are now built around digital computer systems that manipulate sophisticated, solid-state devices to manage trunk line traffic and routing.

Connections to the trunk lines involve additional equipment, the switch (SSP), referred to as *transmission equipment*. Transmission equipment concentrates the communications load to maximize the capacity of the trunks. Transmission equipment also includes

devices such as digital and analog multiplexers and de-multiplexers and packet switching. Packet switching divides a message or conversation into discrete "chunks," and sends them to a destination sometimes using different physical routes. The "chunks" are reassembled at the final destination. Packet switching and multiplexing are both methods for maximizing available trunk capacity when moving voice and data traffic.

Telecommunications Equipment

Landline Equipment

Today's telephone switches are nothing more than expensive computers with sophisticated software that direct voice and data and provide features such as call waiting, caller ID, voice mail, etc. Therefore, the equipment exposure is the same as for any other computer or sensitive electronic equipment. High temperatures, moisture, air contamination, and electrical surge are the greatest threats. However, the telephone industry recognizes the critical role these devices play in their networks. Therefore, switches are manufactured with stringent specifications that define a rigid and extensive set of performance, quality, environmental and safety requirements.

In addition to switches, telecom systems contain devices that are similar to computer hard drives. These devices contain logic that allows the system to store telephone calls and create the billing data used to prepare telephone bills.

Typically, switches, which range in price from $1-10M, do not experience catastrophic failures that require they be replaced. If the switch does experience a hardware failure, it is usually corrected by replacing a board or card that ranges in cost from $3,500 to $10,000.

Since the foundation of telecommunications equipment is electronic components, the greatest equipment breakdown threat is excessive heat. Heat can cause electronics to fail and may ultimately lead to a fire. Since the central office where these switches are housed would typically be equipped with fire sprinklers, a fire to one switch could lead to losing all the computer equipment once the sprinklers turn on.

There is a long lead-time (several months) for purchasing telephone switches. -And, one manufacturer's switch is not interchangeable with another's. Because of the cost associated with this equipment, it is not typical to find spare switches sitting around a central office. However, in order for the network to be redundant, switches are typically only loaded to about 40% capacity (max). Therefore, any given switch can pick up additional load if another switch fails. Manufacturers of switches include:

- Lucent
- Nortel
- Siemens
- Cisco
- Alcatel
- Fujitso
- TelLabs

- NEC
- Ericsson

Cellular Telephony

Wireless (cellular) communications, contrary to its name, is not completely wireless. In fact, the only part that is wireless is between the handset (cell phone) and the antennae at the cell tower. Once the signal is received at the cell site, it is sent along the same landline network as traditionally phones. Therefore, the equipment breakdown risk is essentially the same, with the only additional exposure being the transmitter/receiver equipment and antennae.

Cell sites are typically spaced one to 16 miles apart, depending on the geographical terrain and customer density. In cities, cell sites may be only blocks apart. When a cell phone is turned on, an RF (radio frequency) signal containing your location is sent out to nearby cell sites. When a call is placed or received, the cell site with the strongest signal and available traffic will handle receiving and transmitting the call. As you pass from one area to another, the cell sites communicate with each other (via a network of hardwired computers) and transfer control of the call to the site with the strongest signal and availability.

Each base station antennae system is linked to a switching and control office called a Mobile Telephone Switching Office (MTSO), which may or may not be located in a local telephone company's central office. The physical links are high-capacity circuits that carry calls (and data like e-mail, stock quotes, Internet, etc.) and control information between the MTSO and the base station. Besides switching calls between the telephone network and other mobile network base stations, the MTSO:

- Tracks the location of the mobile unit within the cell area;
- Directs the hand-off of the mobile unit from one base station to another;
- Locates a mobile unit when an incoming call is to be received;
- Performs accounting for the call (call duration, roaming, etc.).

Wireless cell sites have the same type of exposures as landline central offices. The main difference is that a cell site has radio frequency equipment (antennae, transmitter, receiver, etc.) not found in the landline network. The additional risk at a cell site is external damage to the tower or antennae.

Telecommunications Infrastructure

It's useful to examine the infrastructure supporting an e-business and to note the ramifications of equipment dependencies. Figure 3 shows that each successive layer of the pyramid is dependent upon all of the layers below it.

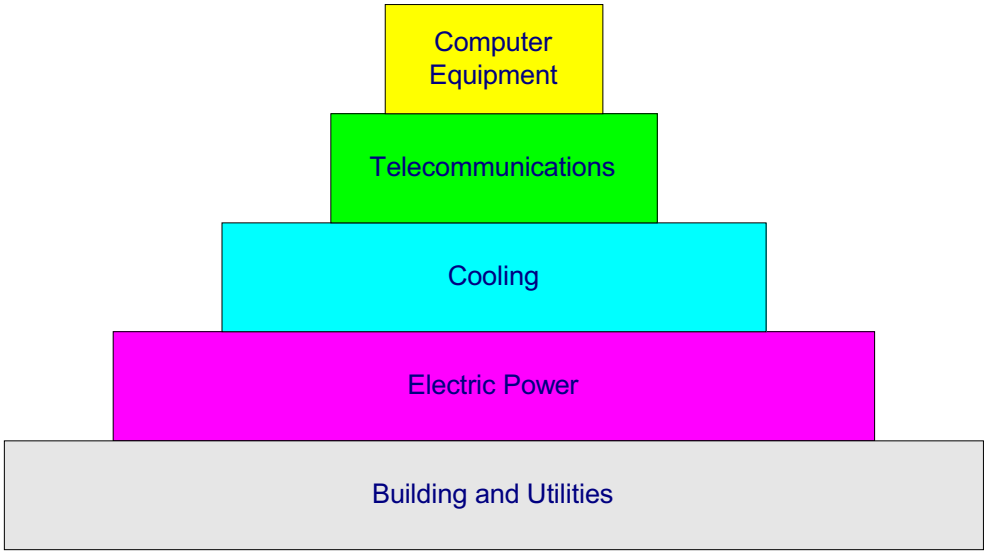


Figure 3

Building and Services

Both equipment and infrastructure elements are usually installed in substantial buildings having extensive physical security and fire resistant construction. Such a structure forms the base of the infrastructure pyramid in the figure. We often tend to take buildings for granted, but they deserve some special respect in this case because of the protection and support they provide for this industry. Not only are telecommunications vital to fire and safety services, they are also important national assets, and can be the target of terrorists or anyone bent upon inflicting damage. A robust, solidly built structure with well-designed security and alarms is an important layer of protection against many kinds of intruders. Risks not characterized by this caliber of shelter for vital equipment cannot be considered equivalent, even if equal in other respects.

Routine maintenance and testing of Heating,Ventilation and Air Conditioning (HVAC) and emergency power systems are very critical. Good locations have well documented procedures and records of maintenance activities and test results. In periods of tight budgets, there may be tendencies to shortcut these activities since much of this may be done by outside contractors.

While failure of the HVAC system is probably the greatest threat to a complete switch failure, building age is another concern . Very often, cable trays, which are attached to aging concrete walls and/or ceilings, are routed directly over switches. If the anchors supporting these cable trays become loose, the switches can become damaged from the falling cable and trays.

Electric Power

Ascending one layer, we come to the next vital layer of infrastructure, namely the electric power supply. Power supply for telecommunications enjoys the benefit of a long tradition of reliability built into the public telephone network.

The electronic equipment operates on very clean Direct Current (DC) provided by batteries that support the electronic equipment for several hours in case of complete power system failure. In addition to the reliability these batteries provide, they also protect the powered equipment from electrical noise prevalent in alternating current AC systems. Rectifiers convert commercially available AC power into DC power, which is used to charge the battery system and operate the system under normal conditions. When the AC power fails, emergency generators powered by internal combustion engines or combustion turbines supply the AC power. This will usually recharge the battery systems in the event of an extended power outage. A primary benefit of this arrangement is that power from an AC generator can be rectified and used without any concern for switching interruptions to the load. This prevents unacceptable voltage or frequency fluctuation — not a trivial matter with sensitive telecommunication equipment.

Routine maintenance and testing of the entire power system is extremely important. It is critical that all main electrical connections be checked regularly to ensure the integrity and cleanliness of the system. Equally important is assuring that fuel for the back-up systems is well maintained and adequate. Extended power outages will require refueling on a regular basis.

Power outages are not uncommon for many reasons. Each year there are some instances of service outages caused by emergency generators that don't perform correctly during power failures. It is very important that the entire power system be equipped with alarms and monitoring systems that can monitor critical and remote locations.

For example, most system outages attributable to power are caused by improper operation of the emergency power generation systems. Remote locations, that are inaccessible during extreme weather conditions, have run out of fuel. Direct damage to such equipment can be small; however, the Extra Expense and Business Interruption loss experienced can be significant.

Power requirements range from 10 kW to several thousand kW in central offices and 2.5 kW - 24 kW in remote locations. Generally, emergency generators support HVAC and other computer systems (in addition to the telecommunications equipment) when operating centers are located in the same building. Therefore, routine maintenance and testing of the entire power system is extremely important.

As a rule of thumb, emergency generation systems operate between 50 percent to 80 percent of the designed load, and are replaced with larger units when the load reaches 90 percent of designed load. The life expectancy of this equipment ranges from 15 to 30 years. Diesel-powered generators have the longest lives. Combustion turbines have shorter lives and, at times, require spare parts that are difficult to obtain for maintenance. The following are some typical examples of emergency power installations:

Office size	Generator	Capacity	Load	Center Description
50,000 lines	4 Diesel 2 - 1500 kW 2 - 2000 kW	7000 kW	4300 kW	Major urban center offices and operations centers included
30,000 lines	2 Turbines 2- 2000 kW	4000 kW	3000 kW	Suburban center equipment only
25,000 lines	1 Diesel	750 kW	450 kW	Small urban area offices and operations
2,000 lines	1 Diesel	40 kW	12 kW	Small town equipment only

Generally, a location will fall into one of the above categories. However, there may be local differences that must be taken into account. For example, some of the centers in New York, Chicago or other major metropolitan areas, may require much larger units.

Cooling

When electronics are clustered in a compact area heat can build up and put the telecom equipment at risk for damage. Therefore, telecommunications equipment should be installed in an environment with adequate cooling.

In addition, the equipment must be designed to meet the heat density and dissipation required to match the building's installed equipment. This is a very important consideration when introducing new equipment into a location. As a result, you will find in many cases that the system was designed with excess cooling capacity to handle this exposure.

Failure of an HVAC system may result in catastrophic damage to telecom equipment. Most equipment will operate reliably up to 90 degrees Fahrenheit. However, HVAC systems and buildings should be equipped with alarm sensors that are designed to shut down telecommunication equipment when temperatures exceed a certain temperature. In addition, it's important to change filters regularly to protect the electronic equipment from contamination.

Routine maintenance and testing of HVAC and emergency power systems is critical. Good locations have well documented procedures and records of maintenance activities and test results. When budgets are tight, many tend to shortcut these activities to cut the costs of outside contractors. In the long run, however, cutting maintenance budgets puts one at risk of costly losses.

Telecommunications and Computer Equipment

Much of the equipment used in the telecommunications industry is specialty computer equipment. Successful operation of telecommunications equipment is entirely dependent on an infrastructure that comprises things like electrical power and mechanical cooling. It is recommended that the risk analyst follow this approach in examining an individual telecommunications risk.

Telecommunication facilities often have extensive self-diagnostic and monitoring systems that report operational status, individual component failures, and loss of power or environmental control (heating or cooling). Most system cards switch to a spare circuit when a line indicates a failure is eminent.

Good locations have alarm systems with remote monitoring of all critical system functions. The switching and transmission system hardware is very reliable, and is designed to detect and correct errors or switch to spare circuits when necessary. Except for individual line cards, the switching equipment is duplicated with approximately 50% of its software and processing power being directed to diagnostics and testing activities. Almost all troubles are detected and corrected before they affect customer service. Switching systems are remotely monitored in Switching Control Centers around the clock, 365 days a year. All alarms for all switching systems are displayed in the control center. Failures are generally caused by software or human errors. Equipment failures are generally limited to small switching components such as line frames or line cards. Fires, floods, volcanoes, earthquakes, espionage, terrorist attacks and other natural events can cause catastrophic failures.

What Can Go Wrong?

The facilities of the telecommunications industry are generally robust, well engineered and highly reliable. The facility, combined with the inherent redundancy of the public switched telephone network, leads to an extremely reliable and flexible system. This reliability can be demonstrated by the loss of a major network location at the World Trade Center on Sept. 11, 2001. Serious interruption of regional telephone traffic was not experienced. Telephone networks in the industrialized world are truly dependable.

However, there are risks, and equipment losses can occur. But, the frequency of such events may be significantly lower than what might be expected in other industries that rely on electronics. Even when equipment failure does occur in the telecommunications industry, business interruption is rare. In most cases, an equipment failure temporarily reduces the traffic capacity of the switching or transmission equipment. And, the equipment is designed to continue operating while repairs are being made.

Replacement Values

The cost to acquire telecom equipment is a good gage to measure potential loss severity. While it is extremely unlikely that an entire telephone switch could be taken completely out of service, short of an event such as the attack on the World Trade Center, it is always wise to know the real replacement value of insured assets. As a rule of thumb, a telephone switch should cost about US$60 per line. That is to say that a 10,000-line switch will cost about US$600,000 to replace.

An equal amount on a per line basis should be recognized to cover replacement of transmission equipment. Together, a 10,000 line central office represents about US$1,200,000 in switching and transmission equipment. This number of lines is probably what one would expect to see in a modest size urban or suburban central office.

Property Damage

The most serious property damage loss scenario would involve loss of cooling in a period of hot weather. High temperatures are the enemy of electronics, and extended exposure to high temperatures will lead to failures. The extent of these failures determines whether a significant property damage loss will occur. Even when fairly extensive damage has been inflicted, the highly modular nature of telecommunications equipment should enable restoration of full capacity by replacement of affected modules or circuit boards.

Power loss is not likely to be a serious threat to telephone facilities. This is because of the underlying DC power systems that support the electronics. Even in cases where power is lost by failure of backup generation and battery depletion, it is unlikely that the equipment will be damaged when operations are resumed.

Business Interruption

Business interruption involving telecommunications is difficult to anticipate. Network redundancy mitigates any significant overall loss of business. The telecommunications network is not monolithic. It's possible that a loss in a facility may significantly reduce one company's earnings while increasing income for another. It is entirely possible that a company suffering from an equipment failure at one of its locations may actually result in a windfall of revenue to another company whose facilities may be called upon to handle the re-routed traffic during the outage.

Underwriting Consequences

Insurers must know the size and type of the risk anticipated. There is sufficient variation in the industry to make general rules inapplicable. For example, ownership of exotic communications assets such as a satellite will require special attention to coverage intent and loss potentials.

Unusual situations may be encountered. There are companies that perform rather specialized functions not ordinarily associated with telecommunications. An example would be a company performing control and telemetry for an Arctic petroleum pipeline, and having a backup trunk carried on a satellite uplink/downlink. Such a company would not benefit from redundancy that is characteristically found in a public switched network. The loss scenarios possible in and the potential consequences of equipment failure may be very substantial for both property damage and business interruption.

Obsolete equipment should be examined to review its condition and whether replacement parts are available. Replacement parts must be taken into account by underwriting, because lack of parts makes any loss more serious.

Contracts define the relationship between telecom companies and are an important element in assessing potential business interruption exposure. When a geographically limited firm is involved, the impact of a single outage at one of its facilities can have adverse business interruption consequences that might not have occurred had it owned a greater portion of the total network.

All telecommunications facilities are a potential target. Whether in war or in a terrorist attack, telecommunications represents a vital infrastructure that an enemy would be anxious to deny to an opponent.

The critical equipment in a telecommunications facility need not be the telecommunications electronics itself. As in other e-businesses, the supporting infrastructure can be more important in terms of loss potentials. Electric power, heating, ventilation, and air conditioning is frequently just as vital to overall function, and failure of even individual items can cause extensive property damage. It is advisable to learn whether this infrastructure is designed and installed in a manner worthy of telecommunications reliability.

Legacy Equipment and Industry Forecasts

The current vintages of telecommunications switching equipment include the No.4 ESS and No.5 ESS manufactured by Lucent Technologies, the EWSD from Siemens, and the DMS 100 and the DMS 100/200 from Nortel. The No.4 ESS is no longer manufactured and the others are mature and fully developed switches. They are deployed throughout the Telco and Long Distance carrier networks. There are some No.1 ESS machines still working in the local exchange networks. This equipment is also no longer manufactured. These machines were first deployed in the 1960s and are well beyond their technological ages although they still provide excellent service. Currently, there appears to be no problem acquiring replacement parts for equipment failures of any of this equipment. In the United States, the Regional Bell Operating Companies have very active Plug In Inventory Control systems. Defective plug-in circuit packs are returned to various vendors for repair. Also, as older equipment is replaced in one office, it is transferred to other offices to accommodate growth. At this stage in the technical lives of all of the switching equipment mentioned above, manufacturers are not spending a lot of resources on further development but are looking forward to the next generation of switches.

The next generation of switches will be ATM (Asynchronous Transfer Mode) and/or IP (Internet Protocol) based switches. This equipment is now in development with some early models deployed in carriers' laboratories. The first deployments will be installed in tandem in the local and long-distance networks. This will occur in the next two to three years. Installations in local-exchange networks will probably begin in the next three to five years.

Part 2 — E-Business Risks

Definition

An e-business risk exists at any commercial business location that produces revenue based on transactions executed by means of a public or private information network. The individual transactions may be large or small. E-business locations present unique exposures to property, liability, and equipment breakdown insurers, as compared to those presented by so-called "brick and mortar" business locations of similar physical size. The transactions involved in e-business can include retail sales, currency and securities trades, credit card charges, or information services. In most commercial contexts, an e-business involves an Internet Web site.

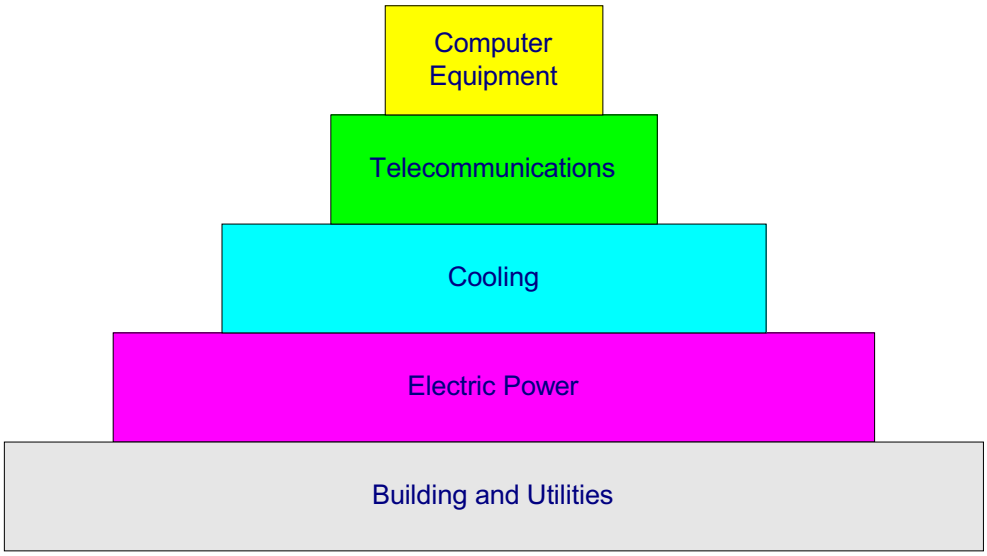
What is a Web Site?

A web site is a virtual storefront. It is similar to a telephone call center with automation. A key difference is that it can operate around the clock, seven days a week. Another is that it can serve a worldwide market.

A web site can be active or passive. In the passive mode, it serves merely as a point for distribution of information. The information can be as minimal as an online business card or as elaborate as an electronic copy of the sales catalog. The key is that in a passive Web site, no transactions can be performed on line.

An active web site offers a two-way exchange of information, usually comprising a sales transaction. An Internet customer can search through the catalog of the e-business and, by simple mouse click, designate products to be purchased. Once the customer has designated all intended items for purchase, a checkout can be accomplished during which the customer provides credit card information and shipping instructions. Development of Internet commerce in recent years has strongly favored the active Web site.

Look again below at Figure 3. The pyramid shows that the basic building block is the building, which provides structure and shelter to the e-business location. On that foundation are successive building blocks in descending order of necessity. Electric power is required by all of the elements laid upon it — cooling equipment, telecommunications gear, and computers. All must be present and properly interconnected for the location to operate. *Each functional block depends on all of those below it in this figure.*



Distinguishing Characteristics - Equipment

The development of the e-business model presents a few (and perhaps only a few) differences from an equipment standpoint.

These arise from two aspects of e-business:

1. Most e-business technology assets are a collection of solid-state electronic equipment items of relatively modest individual component cost. Whether this is telecommunication gear or an Internet server farm, it can be economically repaired or replaced on an individual item basis. Even telephone switches having high acquisition cost are built in a highly modular way and can be readily repaired after *individual* component or module failure. Only an event that damages or disables a significant number of these individual equipment items will generate a really large claim under an equipment breakdown policy. In the telephone switch example, failure of a great number of modular elements is necessary before repair cost could begin to approach the acquisition cost of the switch.

2. Two kinds of events can produce widespread damage or disablement: (a) loss of power or (b) loss of cooling.

   In the loss of power case, business interruption will be the principal loss component, since the hardware should remain intact during the power interruption and be ready for return to service on its restoration.

   Loss of cooling, on the other hand, can produce widespread failures of electronic components resulting from high internal equipment temperatures, leading to costly property damage and ensuing business interruption, which will continue for as long as it takes to restore pre-loss operation.

   Heat kills. A rule of thumb: for every 10 degrees Celsius rise in temperature, the speed of chemical reactions doubles, including the chemical degradation of insulation materials and solid-state transistor junctions. From a technical standpoint, much of this heat-induced damage can be avoided if the facility is designed with interlocks that will perform an orderly shutdown of hardware when there is an increasing temperature. Such interlocking should be mandatory for insured locations.

Property-casualty loss events that involve an e-business site can be exceptionally severe. Such losses are likely to involve destruction of a large number of equipment items. Even though individual values may be modest, the quantity of these that can be installed in a given space can represent an exceptional content value. This is especially true if an ultra high reliability power and cooling installation is included in the loss.

Whether invoked under an equipment breakdown or property-casualty form, business interruption can be particularly dangerous in the e-business world if the location handles a high volume of transactional business. Large Internet retail sales and bank credit card processing operations are examples. What is the dollar value of 20 minutes of transactions for a major credit card? It is technically possible for such operations to be capable of a transaction volume which is at least an order of magnitude greater than that delivered by a state-of-the-art, telephone sales operation of equivalent physical size.

We argue for a new metric called Transaction Density.

> **Transaction Density = theoretical max number of transactions / unit time X average transaction value / floor area.**

While the number so calculated may not match with the actual historical business volume of the location, it will indicate its maximum potential. If reliable values are not available, it would be prudent to limit business interruption coverage at some agreed level that permits rational underwriting.

Internet sales operations are becoming more numerous. It is a class of e-business risk that is growing rapidly. Such businesses do not, as a rule, always employ the kind of rugged power and cooling infrastructure that has been developed over time in the telephone industry. It is these newer enterprises that may not be backed by a sufficiently reliable power and cooling systems, and hence represent a greater equipment breakdown risk.

Computers and Telecommunications

Computers that provide functionality to an e-business can serve as file servers, telecommunications switches, or other network elements. Market forces (competitors) generally require that these be at state-of-the-art level of speed and function. Internet customers are intolerant of the delay and inconvenience imposed by obsolescent equipment and systems. For this reason, these objects tend to be reasonably new and, if the enterprise is financially healthy, constantly supplemented by late model gear.

There is capability for growth built into locations in this class that can be troublesome in the event of a business interruption claim. E-business is defined by automated transactions. Equipment rather than the numbers of sales employees that limits the business transaction capacity of an e-business center. The equipment list is selected and installed in anticipation of the busiest possible day of the busiest possible season. If that is not enough, a significant rate of near-term growth is allowed as well.

When a loss occurs, there may be a tendency to present the theoretical maximum transaction rate as the measure of actual business interruption. Bringing this number down to something real in that situation will be a little trickier than with other business scenarios.

The key to successful underwriting of computer and telecommunications equipment from a property damage perspective is a matter of accumulating good equipment replacement values and tracking loss events, and developing reasonable loss events scenario estimates.

Electric Power and Cooling Infrastructure

When Internet commerce achieves a certain level of importance to a business, it becomes a "mission critical" function. This will occur when even a short duration loss of the revenue stream produced by Internet transactions becomes intolerable. Mission critical status is inconsistent with reliance on an increasingly unreliable electric utility system. Have you noticed that the load on utility power grids has become routine news whenever temperatures soar and demand peaks? The alternative to total reliance on utility power is development of on site power generation in one form or another.

Site power generation can range from a simple standby generator with battery-backed power supplies to a full-scale Random Array of Independent Devices (RAID) type, ultra-high reliability primary power system. When considering the importance of electric power, it is important that cooling be a part of the process. Almost every kilowatt consumed by electronics is released as heat, and that heat must be removed from the electronic devices. The reliability of cooling apparatus must be every bit as reliable as the electric power source.

Map of Mission Criticality

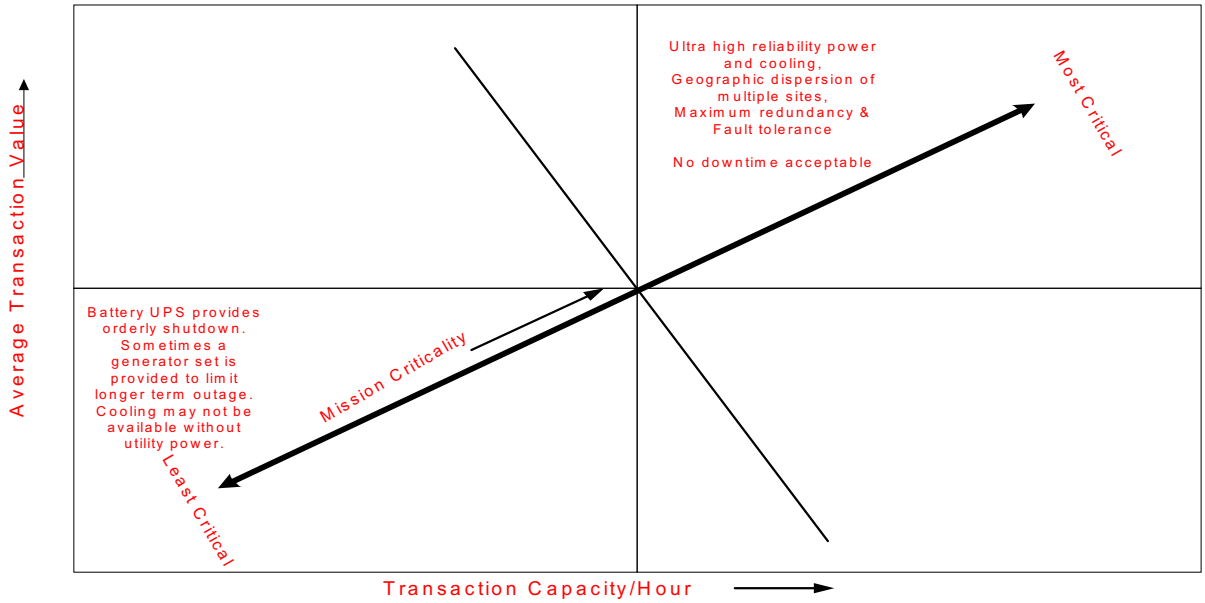


Figure 4

Whatever the type of alternative electric supply, there are additional costs to consider and there are significant new equipment breakdown risks to be confronted. The exposure will be composed of business interruption resulting from lost business transactions. Since Internet transactions can be executed in great volume and quickly, the business interruption potential can be very large.

Successful underwriting of the electric power infrastructure exposure requires development of an accurate replacement cost estimate of the large-value equipment installed in the electric support system as well as an up-to-date assessment of the business interruption potential presented by the associated loss event.

When using the RAID approach to an electric power system, the system represents a very large investment in equipment, sometimes as much as $600 per square foot of e-business space. The good news is that a properly engineered RAID system is extremely reliable, with availability exceeding 99.999 percent. Therefore the severity in terms of business interruption and equipment damage may be substantial, but frequency ought to be correspondingly low.

One last word about a RAID architecture power generation system: these are justified only by the very largest, mission critical e-business locations. They would include large on-line banks, credit card processing centers, major Internet services, and the like. Not every computer backup system qualifies for treatment as a similarly high availability power system.

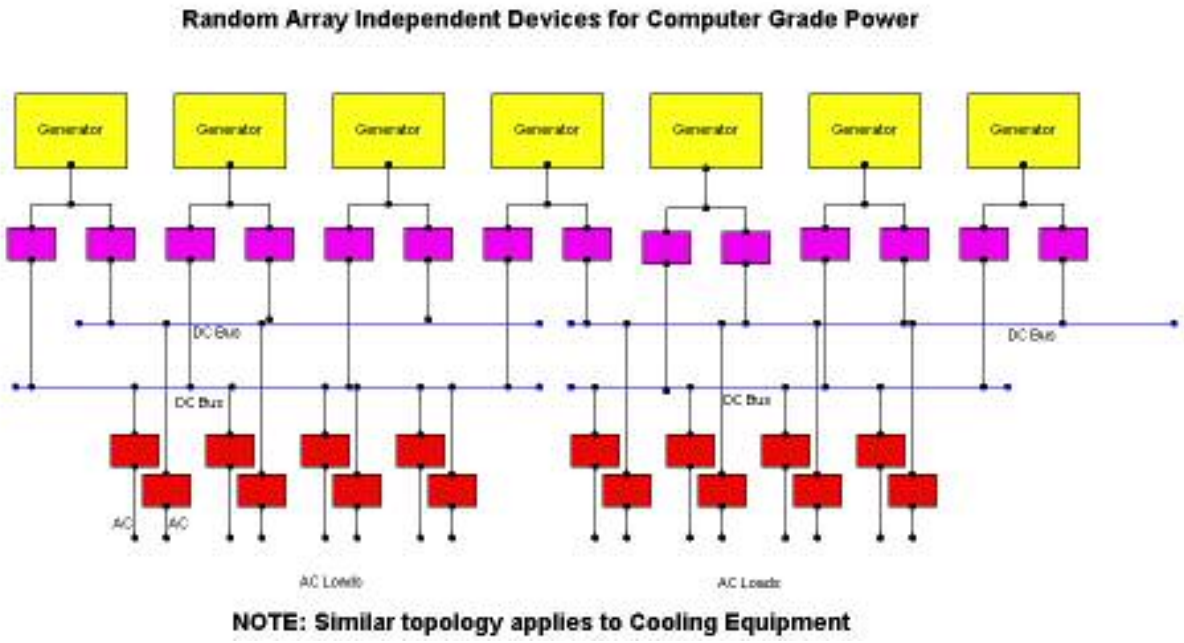


Figure 5

Battery-dependent uninterruptible power systems, even when backed up by emergency generator sets are not in this class, and do not have the same reliability.

What To Do

Underwriting e-business risks require what all other business locations require — sound estimates of actual equipment replacement costs for the most valuable equipment types present. Do not accept "book" values. Apply reasonable loss event scenarios and associated estimates of property damage loss, and, most important, have realistic and up-to-date estimates of business interruption potential.

If there is any one element of the equation that is vital for underwriting success with e-businesses, it is the gathering of this information, combined with knowledge of the business model. Good information leads to good estimates of loss potential, which in turn leads to good underwriting results.

In Conclusion

Telecommunications equipment, while very sophisticated and cutting edge, has a strong record of reliability. The computer electronics that comprise telecom switches and transmission equipment are very durable when housed and operated in a clean, cool and dry environment. Because of the modular design of the equipment, typical failures usually involve replacement of a circuit board for complete repair. And, the redundancy of the network design permits seamless operation of the telecom system even in the unlikely event that an entire switch is lost.

The real threat to high technology telecom equipment lies in the traditional building infrastructure equipment. Since sensitive electronics will not tolerate high temperatures or humidity the integrity of the building ventilation and air conditioning system is critical to the continued operation of computers and telecommunications equipment. A failure to the building's HVAC system is the greatest risk hazard to telecom equipment that is not designed to shut itself down on high-temperature conditions. Similarly, equipment located in a facility with a suspect power system may be at greater risk. Power system failures can impart damaging electrical transients that can destroy the electronic components of telecom equipment. Having adequate system protection and emergency response plans is the best defense against telecom equipment failure.

# # #