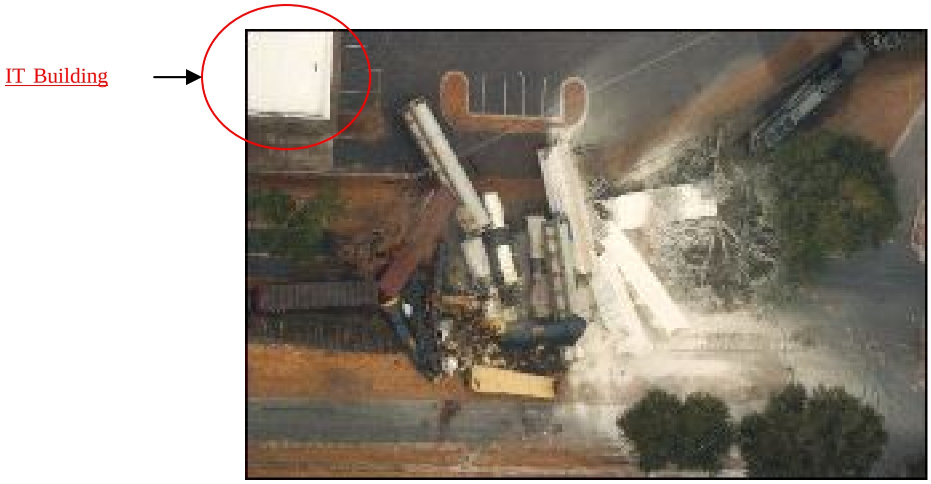
DISASTER *IT*

Peggie Koon
Manager, IS Plant Systems
Avondale Mills

It's every IT director and manager's nightmare. You are awakened in the early hours of the morning by a phone call from an employee who is on-call. You imagine that a system has crashed. She tells you about a call she just received; there's a problem with a warehouse printer. You utter a sigh of relief; then she proceeds to tell you that she is unable to get to the facility. All roads are blocked. You stay on the phone with her as she drives 10 miles via the local interstate highway in an attempt to access the plant via back roads only to be stopped by yet another road block. Finally you decide you need to turn on the local news to see what is going on. You tell the employee to go home because you have just heard that there has been a deadly chemical spill in the area -- No one is being allowed into or out of the area that has now been declared an evacuation zone. You watch the news ever so intently for details…there is a picture of the crash site being shown on television.

According to the news, the crash occurred near one of the company's manufacturing plants. But a closer look reveals that the building that is flashing across the screen is not a manufacturing facility. You recognize that building – it's the ***IT*** building – a building where you and almost every business system server reside, along with associated disk drives that house operating system and business application system software, corporate databases, and more. In addition, the company's communications hubs for telephone, e-mail, Internet, and Intranet services reside there. Indicators are that the chemical gas that caused 9 deaths and thousands having to be evacuated has resulted in the worse imaginable scenario for disaster recovery for your company. All computers in the ***IT*** building are rendered inoperable by the gas; all telephone lines to the company plant sites are down. You want to wake up from what must be a nightmare, but it's impossible… because it's not a dream, it's true!

What would you do? How would you react to the loss? I'm not referring to the loss of life because we all know how tragic such an incident would be. Would you be able to respond proactively to the disaster?   Would you have an executable disaster recovery or contingency plan in place to respond to such disaster ***IT***?



Courtesy Augusta Chronicle Online. Web posted Thursday, January 6, 2005
By Kate Lewis, Karen Ethridge and Jim Nesbitt | *Staff Writers*

Sounds like something that would never happen in a million years, right? Wrong! It happened to all of us at Avondale Mills in Graniteville, South Carolina. On Thursday, January 6, 2005, a northbound train hit a parked train at 2:39 a.m. causing fourteen (14) cars, including three tankers which held 90 tons of liquid chlorine, to derail from the track near the IT building (encircled in the photo above).   At atmospheric temperature the liquid chlorine became a deadly gas that was heavier than air; the chlorine gas permeated every building within a one-mile radius of the crash, destroying shrubbery, trees, and any metallic surfaces that it encountered along the way. Cars that were once running stalled in the middle of nearby streets, fish in a local creek died, electrical switch gears and boxes were corroded, motors and electrical components on machinery at the various plants were damaged, electrical outlets sparked spontaneously, and computers in the company's ***IT*** building came to a silent but immediately discernible halt. No one at the company had ever imagined such devastation could occur and none of us were prepared for the effect that this horrible accident would have – especially relative to ***IT***.

A Ripple Effect

By now you're probably wondering how a company's entire business could be affected by ***IT*** due to such a disaster. Before I begin to explain, let's review our definition of ***IT***.

In my last article, ***"Are You In Control?"*** published in the Management Division January 2005 newsletter, we defined an ***information system*** as the combination of computers and people used to provide information to aid in making decisions and managing a firm.

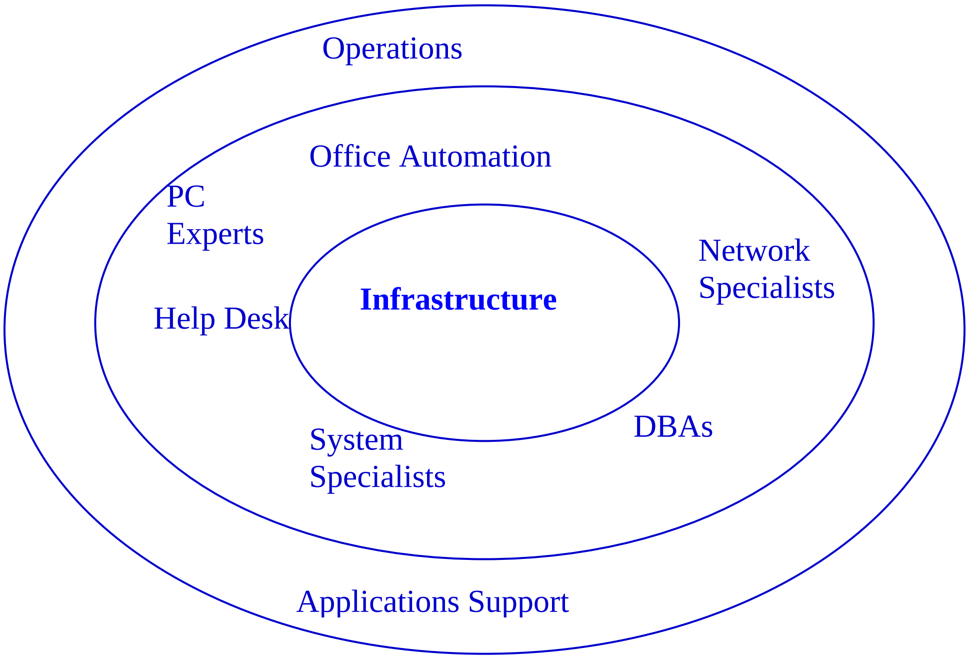
In "***IT Management, Century 21***", ***information technology***, or ***IT***, was defined as an acronym that is used to inculcate in the minds of every level of corporate and middle management the concept that all of the ***computers*** or ***information systems*** in a company – whether they are used at the plant floor or in the board room – are a part of the company's investment in technology.

At the most rudimentary level, then, we can assume that any computer that malfunctions as a result of a disaster is included in disaster ***IT***. For example, a computer controlled drive system on a machine that suddenly fails due to corrosion of the drive system computer or the drive system electronics is a part of disaster ***IT***. A multifunction processor in the plant's process control system, which is used to control the machine's steady state processing that suddenly fails due to corrosion of the boards is a part of disaster ***IT***. Whether it's the computers that are located in an ***IT*** building, as was the case in the scenario above, or the computers at the plant floor – in a control room, on a machine, or on a desk top – when computers and information systems are affected because disaster occurs, the result is disaster ***IT***!

A Recovering Approach

When a company attempts to recover from disaster, the first step usually includes assessing the damage to its ***infrastructure***, which is at the core of its operations.

The next steps include identifying the key people required to get the company's operations back up and running, developing a strategy for restoration/recovery, and implementing the plan. A look at the typical structure of a company's ***IT*** quickly reveals a similarity: like the typical company, the ***infrastructure*** is at the core of the ***IT*** organization. The key people and resources required to support the ***IT*** organization are defined by the ***IT*** infrastructure; hence, the ***IT*** director or manager must take a similar approach towards ***systems*** recovery.



In the above diagram, the ***IT*** organization is an ***IS*** strategy that includes ***all*** *computer systems* in a company, ***all*** *transfer media*, ***all*** *software products*, ***all*** *databases,* and ***all*** *technology providers*. The old expression, "***the network is the computer***" applies when this strategy is implemented. And when disaster strikes ***IT***, it affects every aspect of the operations -- from payroll to customer service, to benefits, to plant floor production, to orders and sales, to inventory and shipments, to decision support and executive information. A tightly integrated ***IT*** organization/strategy is critical to the survival of today's companies; however; such a strategy can increase ***IT*** vulnerability during disaster.

At the infrastructure level of ***IT*** is the communications backbone, or network, which usually includes any voice and/or data transfer media and associated servers. For example, the loss of a company's PBX might affect both internal and external communications. Cell phones can be immediately deployed for people-to-people communications; in the plants, walkie-talkies can be used. If the corporate wide area network is lost, communication between clients and servers is also lost. Communications between systems and peripheral devices (such as printers, thin net and PC clients) that were connected to switches and hubs on the corporate wide area network will also be rendered useless due to the loss of the network. The Internet is often integrated into the business (customer access via portals, e-mail, or internal corporate Intranet users) so that loss of Internet access also affects customer and company communications. The first order of business, then, is to restore the network – both voice and data – so that internal and external people-to-people and system-to-system communications are restored. You see every server in a company is typically connected via the backbone. There might as well be no servers without the network!

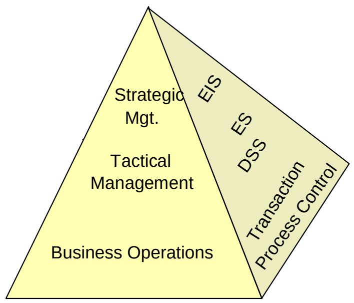
In our case network and system specialists worked around the clock to restore the corporate voice and data networks; the PC and office automation experts worked in tandem with the communications experts to replace PC's and printers that were affected by the disaster. In the interim, a wireless network was established to resume customer communications using an ***ISP*** (Internet Service Provider). Remember we defined ***IT*** as ***all*** *computing platforms* (Windows XP, Windows 2000, Windows NT, OS, OpenVMS, etc.), ***all*** *communications protocols* (TCP/IP, etc.), ***all*** *software applications* (business or process control, process automation), ***all*** databases (DB2, SQL Server, Sybase, RMS, etc.) and ***all*** *technology providers* (DBA's, programmers, analysts, network managers, system managers, help desk personnel, control system engineers, etc.). Every aspect of the ***IT*** organization is affected during disaster ***IT***.

Backup and Restore

When the servers are destroyed, the process of replacing the computer hardware is usually fairly uncomplicated. Suppliers, especially those with whom you ***partner***, tend to make every practical effort to assist in an expedient replacement process.

The real key to the effort lies in the availability of the ***technical IT experts*** and the existence of off-site ***software***, ***system*** and ***data*** backups necessary for server restoration. Notice that the words ***software, system***, and ***data*** are highlighted. All too often companies invest in offsite *backup storage for company data* without considering the need for concomitant *offsite operating system and application software backup storage*. This can be a fatal mistake in disaster ***IT***. When you consider the types of ***IT*** that were discussed in "***Are You In Control?***", every aspect of the operations have the potential to be shut down when servers for business transaction processing, decision support, expert systems, and executive information systems are destroyed.

IS Organization



Courtesy: Post & Anderson

Typically companies have servers that are dedicated to each of the types of information systems depicted above.

The applications for these servers are especially vulnerable if they have been developed in-house or purchased with extensive customization. If the disks on the servers are damaged, as might well be the case, the company's operational systems (*business operations*) may only be partially restored. ***The one hope in such a case lies in the knowledge and expertise of the people – the IT experts who developed and maintained the system must be available to re-create the business processes using whatever information that can be salvaged from the system servers.*** Disk forensic experts are often invaluable in the restoration process.

Distribution's Saving Grace

Another fatal mistake in disaster ***IT*** is the lack of contingency planning. Almost every ***IT*** manager has developed or at least conceptualized a disaster recovery plan.

But what if the recovery plan takes weeks or months to implement? What contingency plan is in place? If the server for payroll is lost and can not be recovered, is there a remote resource available to pay your employees? If the order-processing system fails, will you be able to place orders from a remote site, to locate rolls in the warehouse, to print bills of lading, and make shipments to customers? Will you know your inventory levels and order position? Will you be able to receive raw materials and distribute the materials to the various manufacturing facilities to make products? Will you be able to schedule your remaining operating facilities? These are just a few of the questions that must be answered during disaster ***IT***.

Distributed processing has long been utilized in manufacturing facilities, especially where process control and process automation systems are deployed, to ensure that the loss of computer resources in one facility does not affect the operations at another facility. The use of distributed processing at the plant floor level can be a critical ***saving grace*** during such a disaster. The plant systems located in each production facility are usually autonomous from the business servers; these servers can be used to provide accurate real-time production information to management. The plant systems ***IT*** experts can develop applications, for example, to merge production data with warehouse location data to provide visibility of inventory levels to management, which in turn will facilitate the shipping, invoicing, and order entry processes during the disaster. These distributed plant systems provided valuable ***real-time*** information relative to the state of the company's operations. In addition, the plant systems allow new production to continue to be processed in each of the plants during the recovery period.

Lessons Learned

During this disaster, several critical observations were made regarding disaster ***IT***, the most significant of which include:

- □ ***IT*** is a critical resource that affects every aspect of a company – especially during a disaster (such as the chlorine disaster in Graniteville).

□ The most critical disaster ***IT*** resource is the ***IT*** staff. Without a group of dedicated experts who are available and willing to work diligently for the duration of the disaster plan, recovery is impossible

□ The network is the computer; the communications network is critical to the company's successful redeployment of ***IT***.

□ System, software, and data backups should be completed on a regularly scheduled basis. All backups should be stored at a remote off-site facility.

□ Distributed processing should be considered at every practical level of systems configuration so that a failure of one server at one location does not affect the entire company's operations.

□ Development of an ***IT*** disaster recovery plan is not enough. Every company should invest in a pragmatic contingency plan for ***IT***. The plan should be tested ***before*** a real disaster occurs.

□ Partnering pays. The existence of strong alliances (with customers and suppliers alike) is critical to a company's recovery from a disaster. Partners who are willing to work with you through the recovery process ensure survival during and after the disaster.

It only takes one disaster of the magnitude of the chlorine spill at Graniteville for a company located in the heart of a disaster to underline the importance of ***IT*** to its business.

Risk Analysis

As an ***IT*** manager I learned so much personally from being involved in the disaster at Avondale. It has taken weeks for me to fully grasp the total effect of this event – on us as a company and on our ***IT*** organization. What was achieved to get the company's ***IT*** back up and running is nothing short of a miracle. From my perspective, the following is a list of basic steps that can be used in the approach to disaster ***IT*** recovery:

□ ***Identify the key people required to get the systems back up and running.*** If you're a director or manager of IT, you will probably be called into strategic meetings where decisions are being made relative to recovery from the catastrophe. Just as the company quickly assembled its key/critical personnel, the ***IT*** director or manager must quickly identify the key/critical resources required to restore the company's ***IT***.

□ ***Assess the level of infrastructure damage and implement (or develop) a plan to restore it, especially corporate networks and communications, both voice and data, as quickly as possible.*** Just as the company is about the business of identifying its damage to the infrastructure – buildings, utilities, equipment, etc. – the ***IT*** director or manager must remember that that "***the network is the computer"***; without the network critical business processes can not be effectively performed. While the network is being restored, acquisition of the computer systems, any unrecoverable software, and data can begin.

□ ***Identify the critical systems – core business systems – that must be in place to run the business.*** At the lowest or operational level are the process control, process automation, and business transaction processing systems. Without these systems, the systems at the higher levels (EIS, etc.) are not functional. At the plant level, the process control and process automation systems should be distributed at the various manufacturing facilities. Oftentimes manufacturing facilities are also distributed geographically, some of which may not be affected by the disaster. In such a case, these lower level plant systems can be used to restore many of the company's core business processes even though the company's business transaction processing systems are all located in the heart of the disaster.

□ ***Implement the recovery or contingency plan for the critical systems.*** This step may include the purchase of new equipment, the use of backup data, the recovery of data from disaster disks, the use of remote processing systems at remote sites, or any combination of the above. The better the plan for recovery/contingency the faster the recovery process. Every effort should be made to ensure that the necessary resources, including any required external business partners, are available to implement the plan as effectively and expeditiously as possible.

□ ***Remain focused.*** As each critical business system is restored, new opportunities will arise. An ***IT*** director or manager and the entire ***IT*** staff may quickly become overwhelmed by the tasks of deploying the new systems and responding to glitches and problems that may occur. It is important for ***IT*** management to remain focused on the bigger picture, which is to restore the company's ***IT*** systems in concert with the company's plan for recovery of each of its business functions. To accomplish this task, the ***IT*** director or manager must remain cognizant of management/company priorities; the allocation of ***IT*** resources must be coordinated so that ***IT*** is readily available as each segment of the business is re-synergized. Every resource available should be utilized to ensure that the strategy for disaster ***IT*** restoration matches the company's objectives and targets for recovery of its operations.

□ ***Redevelop the Plan.*** Once the company's ***IT*** has been restored, it is critical that the disaster plan, whether it is designed for recovery, contingency, or both, is reviewed and its strengths and weaknesses are identified.

For the past 20 years, as a part of the company's annual external ***IT*** audit, I have been asked to provide a plan for plant systems disaster recovery. And each year I write 3 to 4 pages about the redundancy of our plant systems. I mention that distributed servers deploying clustering technology are used for process automation. I note that periodic complete system backups are performed and that incremental backups are created daily, all of which are stored at remote locations – offsite from the various plant/manufacturing facilities. I also state that distributed fault tolerant technology is used in our process control system configurations. After the review, almost inevitably I am asked to obtain a cost for a plan for remote/off-site processing capability for each of the plant systems. When it's all said and done, the cost of the extended disaster recovery or contingency plan is usually considered prohibitive.

You see, a comprehensive disaster plan for ***IT*** is viewed like an insurance policy that may never be used. After all it has never happened in 20 years so it probably will not happen now, right? Wrong! ***IT*** disaster ***can*** happen to you. It happened to us. Every company should analyze the risk of having a disaster without a feasible/pragmatic disaster recovery and/or contingency plan. If you're not convinced of its importance, just ask anyone from Avondale Mills. They'll tell you that an investment in disaster ***IT*** is well worth the risk!

Peggie is also authoring a series of articles on how IT contributes to plant production improvements. The first in this series "Are you in Control" appeared in our January Newsletter her next article will be in the June 17th issue.

About the Author

Dr. Peggie Ward Koon has over 25 years of experience in developing IS systems for plant process automation and process control; she is an author of technical articles and publications. She has authored nine technical publications, including "CIM Capitalizes on Distributed Controls", ***InTech*** Magazine (1995), "GAMMA -- Graniteville's Application Modules for Manufacturing Automation", ***IEEE Transactions on Industry Applications*** Magazine (1995), "Managing More With Less -- A Real-time Example of Optimized Resource Allocation", ***ISA Transactions*** Magazine (1996), "Textile firms automate to survive; here's how Avondale Mills does it", ***InTech*** Magazine (1998), "IT Management: Century 21, ***Industrial Computing*** Magazine (2001); Industrial Computing Online (2001), and a variety of articles on issues in textile manufacturing including partnering, process automation and process control, SPC/SQC, and IT management for such organizations as the Instrumentation, Systems, and Automation Society (ISA) and the Textile Fiber & Film Industry Applications Society of the IEEE. She is currently a Manager of IS Plant Systems at Avondale Mills in Graniteville, S.C. Dr. Koon is the Membership Chair for the Management Division of ISA, a Senior Member of ISA, and a member of the IEEE.

Dr. Koon is a General Motors Scholar and Graduate Fellow; she received her undergraduate degree from Smith College (Northampton Massachusetts) and has completed graduate studies at Georgia Tech (Atlanta, Georgia) and Kennedy-Western University (Cheyenne, Wyoming), where she received her doctorate degree in Management Information Systems.