PROTECTING THE COUNTY'S ASSETS

Summary

This report is a companion report to "A Disaster Waiting to Happen," first released in April 2005. That report examined the extent to which the county, its cities, and the Sheriff's Department had consistently embraced the state-sponsored Standard Emergency Management System (SEMS). This report, by contrast, examines the extent that certain agencies in which the county has a major stakeholder presence have an adequate disaster management and business recovery process in place. It also examines departments directly under the control of the county or the Sonoma County Office of Education (SCOE). Exhibits C and D at the end of the report contain a brief description of the basic principles of disaster recovery and business resumption, and a glossary of terms.

In the private sector, CEO's and Boards of Directors have specific legal responsibilities regarding control and protection of enterprise assets. In the late 60's, following a major scandal involving bribery by Lockheed Corporation employees, legislation was introduced to make top management of corporations more accountable. The 1971 Foreign and Corrupt Practices Act charged corporate management with exercising close control over the protection of company assets. The penalty for failing could be a prison sentence. In addition to obvious aspects of asset management, it was widely interpreted that the corporate investment in data processing needed to be protected. Many businesses have put in place formal disaster management and business resumption processes. These processes provide recovery for lost or damaged data, critical computer system and network components, and in some cases, loss of key people. They also detail the steps required for a business to get back to normal following a major loss of computing facilities.

While this Act does not apply to local government, it is likely that taxpayers would expect that elected and appointed officials in local government would implement a similar level of control. Indeed, Government Code Section 25000[1] indicates that, among other responsibilities, the Board of Supervisors:

- Oversees most county departments and programs
- Controls county property
- Manages public monies.

Further, the powers, duties and responsibilities of the County Administrator mandate that he/she:

- Advise, assist, act as agent for and be responsible to the board of supervisors for the prompt and efficient administration and execution of all aspects of county government over which the board exercises control and direction, and shall oversee the faithful execution of the ordinances, orders and regulations of such board
- Oversee all central administrative services and supervise department heads of the County's General Services, Data Processing, and Public Information Departments.

In deciding to assess effectiveness of the disaster management and business resumption, the 2004-2005 grand jury selected a representative sample of departments and agencies, as follows:

- Information Systems Department (ISD)
- Tax Collector

[1] California Government Code – Section 25000

- Sonoma County Water Agency ("the Water Agency")
- Sonoma County Office of Education (SCOE)
- Sheriff's Department.

Reason for Investigation

As in many local governments and businesses, most of the county's business is supported by computer systems, both for record keeping and major financial transaction processing. The 2004-2005 grand jury determined that an investigation of the county's ISD data backup procedures was timely. In addition, the grand jury decided to investigate a major revenue department - Tax Collection. This department is heavily committed to use of computers, and might be exposed if disaster management and business resumption planning were not in place. The Tax Collection department is just one example. All of the major county departments financially oriented or not, need to think through the impact of a disaster and the specific steps that would be required to get their business back to normal.

As part of the companion investigation, "A Disaster Waiting to Happen," the grand jury interviewed key senior people and planning staff in the Water Agency and the county's schools. These two agencies have embraced, or will be embracing, the Standard Emergency Management System methodology. However they were not specifically included in the earlier report, since the focus there was the relationship between the county and city SEMS-based plans.

Similarly, the Sheriff's Department was included in the earlier report investigation, but mainly with regard to the agency's role in a disaster external to the agency. For this report, the grand jury examined the effectiveness of the agency's internal disaster management and business resumption in the event that the Sheriff's Department suffered a direct emergency.

Background

SEMS does not prescribe a methodology for managing the effect of disasters internal to county departments and agencies. However, two of the agencies investigated, the Water Agency and the Sonoma County Office of Education (SCOE), do have commitments to a SEMS-based approach.

The basic disaster planning that exists in ISD dates to an era before server-based major networks were developed. It consists of little more than taking copies of critical files nightly and moving them to an off-site location.

The Water Agency is committed to SEMS because it is a major player in many of the types of disaster that could impact the county at large. For example, earthquakes, floods, or damage to water lines. The agency is a key member of the SEMS-based partnerships in the county and currently represents all utility suppliers on the Sonoma County Emergency Council.

As part of the "A Disaster Waiting to Happen" report, the jury interviewed key Water Agency management and planning staff. The jury decided to include its findings and any recommendations on the Water Agency's disaster planning in this report.

The school community in Sonoma County has a grant to develop coordinated disaster management plans, using SEMS. The initial incentive is the same as for the county and the cities, namely that Federal and state aid, FEMA-like reimbursement of disaster and disastermitigation expenses, will be dependent on the schools' commitment to SEMS. There is little doubt that SEMS offers a much-improved planning base.

In the process of investigating the Sheriff's Department regarding its role in external disasters an obvious step was to examine the department's planning in the event of a disaster that impacted the department directly. The Sheriff's Department has a considerable investment in computers, including those in patrol cars. This investment will grow and become an even more essential part of the operation. The investment and other key infrastructure elements need to be protected by a sound disaster plan, and the Sheriff's Department clearly needs an aggressive business resumption strategy. It cannot operate on the basis that it may remain intact through every disaster that befalls the county.

Investigative Procedures

1. The grand jury interviewed key staff in various positions within the agencies and departments as shown in Exhibit A at the end of the report.
2. Tours were made of the following facilities:
    - Information Systems Center
    - Sonoma County Water Agency
    - Dispatch Center – Sheriff's Office
    - County Jail and North County Detention Center.
3. Documents reviewed are shown in Exhibit B.
4. The grand jury attended a test of the ISD file recovery process, using tapes that had been stored off-site.

Findings

<u>Information Systems Department</u>

F1. ISD has an arrangement with a supplier with offices in San Mateo, whereby tape copies of major files are taken each day and stored at the supplier's location. This arrangement does not include files from the school data processing system, for which ISD only provides facilities management.

F2. Files for the schools' data processing system are backed up daily and stored at Sonoma County Office of Education.

F3. The ISD network is well designed with very little "hardwiring." Thus, it is close to providing facilities whereby "anyone, with the right authority, and the right equipment, can get to any application or service." This flexibility should bode well in the disaster planning.

F4. ISD is presently developing a plan to identify the critical points of failure in the data center and the county network, especially those points of failure that have no redundancy. Since this plan is in its early stages, the grand jury expects that any recommendations made in this report can be folded into the emerging plan.

F5. The recovery test that the jury participated in (as observers) was straightforward and the minimal numbers of users involved were able to log on to the "recovered" system. However, the validity of the test was somewhat undermined by using the incorrect tapes! The test facilitator was able to declare the test successful by taking account of the modified steps needed to utilize the recovered data.

F6. ISD tried the conventional approach of attempting to get its major users to reach consensus on which applications would take priority in the event of a major and prolonged outage of the computer systems. Like many other IS departments, they found the responses lackluster at best.

F7. ISD is run on a full cost recovery basis, i.e., its expenditures are funded by charging user departments for their share of the computer usage, basically an equitable scheme. However there is no place in the cost recovery system to separately fund any unique expenditures for disaster recovery plans.

Tax Collector

F8. Most of the computer applications used by the Tax Collection Department are developed by and purchased from a third party provider and are server-based. Sonoma County uses the same applications as Napa County and other counties within a reasonable distance. There is a valid assumption that in the event of a total system loss, the Tax Collection systems could be processed elsewhere, likely at the Napa County facility. The arrangement is reciprocal. It is not clear whether the Tax Collection Department would literally use the copy of the application that resides in Napa. It may be safer to make a copy of the application code in use in Sonoma County, and take it to Napa County when needed.

F9. The Tax Collection Department is not actively involved in periodic testing of the backup and recovery processes for the main systems used. Rather, the department relies on information provided by the supplier of the software or minutes from a user-group meeting.

F10. Tax Revenue is 40% of the county's total revenue, collected at two calendar points, mid-December and mid-April. These two collection points account for 85% of the tax revenue with December being the larger of the two. If a disaster were to take out the system at a point, say December 11, substantial revenue and investment opportunities are at risk. Other than the obvious step of moving the application to Napa, there is not much detailed thought given to the full business resumption (getting back to normal) after a disaster. As an example, after the Loma Prieta earthquake, it took Alameda County some four months before everything in their system usage was back to normal.

Sonoma County Water Agency

F11. The Water Agency has a well-written disaster and recovery plan, dated September 1998, with a revision in process. The jury was impressed to see that many employees, including the General Manager, had designated equipment/water line checking responsibilities should a disaster occur, and typically carried plans and checklists with them at all times.

F12. The Water Agency has an impressive set of business resumption steps in its plan, including a realistic attempt to show how some employees will be working modified hours to help resolve and contain the disaster and some employees will be taking care of normal business.

F13. While this finding is shown under the Water Agency, it applies to almost all of the checklists shown to the grand jury. Many of them read like a cross between *Assigned Duties* and a *Position Description.* Usually the key actions to be performed in the immediate wake of the emergency could be identified, but non-urgent tasks were interwoven (e.g. read document *abc,* complete form *xyz)*. Checklists were rarely broken down by time periods, e.g. first hour, hours 2-4, hours 5-8, first 24 hours. In most cases the checklist was on full 8 ½ by 11 paper with no attempt to make it a portable field usage item.

Schools

F14. There is a grant from the US Department of Education, known internally as "the USDOE grant," which provides for the county schools, including private schools if they wish to participate, moving to a SEMS-based layered set of plans, school > school district > Sonoma County Office of Education (SCOE). The grant does not provide for any equipment, such as generators for remote schools. The layered plans will also highlight the points in the disaster management where the schools would invoke assistance from their adjacent cities (SEMS-based of course) and the cities in turn would know when to invoke county level assistance. The jury believes this to be a challenging but extremely valuable project. All school district superintendents are targeted to have completed SEMS-based plans by March 31, 2006, the grant completion date. Since the grant itself was late in actual availability, that date is already under pressure. The roll-out plan is impressive, providing workshops, training, and disaster plan templates and a survey of equipment inventory and needs.

F15. The pre-USDOE plans that the jury examined, in contrast to the core approach SEMS uses for any disaster, usually treat each individual type of disaster as a separate entity. This has the effect of providing much repetition, which makes each plan indigestible. This is not a good feature for a plan intended to provide real assistance in the event of an emergency. These plans were an outgrowth from "Safe School" initiatives, somewhat dominated by the Columbine School disaster, April 1999, where two students shot and killed 12 fellow students and a teacher.

F16. In the existing pre-SEMS plans, the role of SCOE if a specific school or school district should incur a major disaster is unclear.

F17. Since disaster and security often go hand in hand, the jury is concerned at the truly open nature of the SCOE main office. The SCOE organization prides itself on its service to the community, both the school community and the county at-large, and encourages many visitors. The visitors may be attending a SCOE-hosted event, using the technology center, or attending a non-SCOE meeting. Since there is no security badge system, or formal check-in/check-out process, it would be very difficult to establish the transient headcount in the event of a disaster or evacuation.

F18. In September 2004, following the hostage situation in the Beslan school in Russia, the US Department of Education issued a letter to all school districts and schools, specifically asking them to check certain aspects of security, and clearly expecting them to respond with corrective remedies where necessary. No interviewee that the jury met showed initial knowledge of the letter, although some found it later. In no case was the jury provided with any evidence of a response.

F19. While not yet realized, the USDOE project team is exploring new methods of universal parent contact.

F20. As part of the USDOE roll-out, the project is issuing questionnaires to all school districts and schools to update the communications equipment directory.

F21. During the summer of 2005, the USDOE project hopes to use the American Corps volunteers at the schools to identify all hazardous equipment, furniture, artifacts and shelving.

Sheriff's Department

F22. As this investigation began, a written plan for operating a severely damaged Dispatch Center was not in existence; nor was there an exhaustive written plan for continued operation if the Dispatch Center should be totally lost in a disaster. The grand jury was pleased to see a well-written plan emerge during the study.

F23. As well as the Dispatch Center, the Sheriff's Department has other technology bases that are critical to its operation (or will increasingly be so). The "A Disaster Waiting to

Happen" report noted that the current radio network design had a good level of redundancy and more was in the planning stage. The report also noted that the Sonoma County Law Enforcement Consortium (SCLEC) was housed on a single computer system that was a single point of failure, and a plan is needed to reduce that exposure.

F24. The Sheriff's Department has the capability to develop internal systems for use by the deputy sheriffs. ISD is not involved in the development of such systems, but it may well house the equipment on which they are based. The backup and recovery of such systems is not visible to ISD, unless the Sheriff's Department specifically requests it.

F25. The grand jury was shown the evacuation procedures for the main detention facility and the North County Facility. The grand jury found these procedures to be well constructed with a real attempt to separate the different scale of damage a disaster might inflict.

<u>General</u>

F26. As the grand jury uncovered in the "A Disaster Waiting to Happen" investigation, much of the detailed work in the disaster planning is done by a few dedicated mid-level staff people. This quickly leads to introspective approaches by the planner. Senior management is not providing the continuous effort to ensure that communication with the major stakeholders and junior staff is intensive and frequent.

F27. With regard to county departments, neither the Board of Supervisors nor the County Administrator calls for a periodic review of the disaster recovery nor business resumption plans.

Conclusions

With the exception of the Water Agency, there is a lack of "push" from top management, either elected or appointed, demanding that effective disaster recovery and business resumption plans be in place for the major departments and agencies.

ISD is on the right path and has already done a significant amount of planning for a new disaster recovery plan. This will need funding, and the major users need to take a much more proactive role in the realization of the plan. Effective disaster plans in information technology involve additional expenditures and the user departments need to "club together" and pay for these separately from day-to-day running costs.

That the Tax Collection Department uses standard applications to manage its business is very good news in a disaster planning context; however it can be deceptive. There is a dangerous reliance on the third party supplier's report that the disaster recovery has been fully tested. There is also a dangerous assumption that the application code at the alternate facility is <u>exactly</u> the same as the code normally used in the county ISD. Finding out that it isn't exactly the same at the time it is most needed, is far too late.

The existence of the USDOE grant has most certainly provided some stimulus for the school system disaster planning, ostensibly guided by SCOE-provided staffing efforts. However, the jury wishes to emphasize again that SCOE needs to clarify its role in the invocation of any plans finally put in place.

At the Water Agency, the General Manager and his staff are putting a considerable amount of effort into the agency plan and are taking personal responsibility for parts of the plan. Once the current update is complete and the checklists are fine tuned, this plan will be in good shape.

When the grand jury began investigative work with the Sheriff's Department, there was some surprise expressed that internal disaster management and business resumption processes needed to be well documented. The jury was pleased to see the emergence of the Dispatch Center Emergency Plan during the course of the study.

In all cases the planning work done so far is basically driven by caring mid-level staff people. It is extremely difficult to do good disaster planning and business recovery planning from the "bottom up." Senior management needs to be continuously involved in the setting of priorities and provision of funding when it is not available from grants.

Successful county disaster plans need more continuous communication between the disaster planning functions, their management, and the stakeholders of the plans. Their buy-in to the plan and its level of effort needs refreshing at every opportunity. The bonds that are formed, and the continuous resolution of mutual misunderstandings, pay dividends when a disaster does eventually occur.

Commendations

The grand jury would like to thank all of the people interviewed for the time and information they generously provided. The grand jury would also like to give recognition to the consistent support provided to the schools' USDOE project by the representative from the Redwood Empire Schools' Insurance Group.

Recommendations

Information Systems Department

R1. Complete its initial disaster recovery plan by December 2005, and request the funding it calls for in time for the 2006-2007 budget cycle. This request should include a change in the manner by which such expenditures are funded, separately from recovery of ongoing ISD running costs.

R2. Involve the major users more closely in the design of the new disaster recovery plan. This may need senior management directives to the major users.

R3. Ensure that the new disaster plan under development includes specific recommendations on:

- The need for user consensus on the system and application priorities, both for protection against failure and sequence of recovery in the event that not all facilities can be restored immediately after a catastrophic outage
- The value of distributing some of the servers (presently clustered) and the use of storage area networks – basically a "let's not put all of our eggs in one basket" strategy
- A "non-stop" solution for the Sonoma County Law Enforcement Consortium (SCLEC) system such that an outage of the main system is instantly switched to a standby, such standby preferably located at a site some distance from the primary location. There are numerous hardware, network and software solutions available to achieve this
- Identify every single point of failure in the data center, including network terminators and cabling ducts, and determine the investment value of providing redundancy.

Tax Collector

R4. Participate more actively, on an annual basis, in the disaster recovery testing of the Tax Collection applications. This should include use of backup data in a real environment, not simply a test to show that the data is being backed up.

R5. Participate, bi-annually, in an actual test, to determine that Sonoma County can successfully process its Tax Collection applications at Napa County's computer installation.

R6. Evaluate the opportunity investment cost of, as an example, a five-day delay in investing the peak tax income in mid-December, and determine what commensurate investment in redundant equipment would preclude the lost opportunity.

Sonoma County Water Agency

R7. Complete the current update of the disaster plan by December 2005.

R8. Modify the existing checklists to be more hands-on, action-oriented, and easier for a disaster worker to carry on his/her person or in his/her automobile.

Sonoma County School Districts

R9. Ascertain whether an extension to the USDOE grant timetable is possible, and determine if an extension would be desirable.

R10. Review the letter from the US Department of Education regarding the Russian school hostage emergency, and expedite action and replies from all school districts.

R11. Develop a pro-forma action checklist for use by all schools in handling post-disaster tasks.

R12. Ensure that the role of SCOE in actual post-disaster scenarios is identified and publicized.

R13. Review the check-in/check-out procedures at the main facility and determine if a change is desirable.

R14. Implement a common parent-contact system as soon as possible.

R15. Complete an inventory questionnaire of school communication equipment.

Sheriff's Department

R16. Work with ISD to identify a cost-effective "non-stop" solution to protect the SCLEC system.

R17. Work with ISD to determine cost-effective backup solutions for internally developed systems.

General (senior management of all the entities)

R18. Ensure that all disaster recovery and business-resumption planning efforts are continuously supported and reviewed by appropriate stakeholder groups.

R19. Require that all county departments file a formal statement of their disaster recovery requirements, for computer-based and manual systems, with detailed descriptions of the necessary steps to return the business to normal.

Required responses to Findings

Sonoma County Tax Collector - F8, F10
Sonoma County Information Systems Director - F4, F8
Sonoma County Administrator - F6, F7, F26, F27
Sonoma County Water Agency - General Manager F13
Project Director USDOE Project - F14
Superintendent of Schools – SCOE F16
Sonoma County Sheriff – F23, F24
Board of Supervisors – F26, F27

Requested responses to Recommendations

None

Required responses to Recommendations

County Director of Information Systems - R1, R2, R3
County Tax Collector - R4, R5, R6
Sonoma County Water Agency – General Manager - R7, R8
Superintendent of Schools – SCOE - R9, R10, R12, R13
Deputy Superintendent of Schools – R11, R14
County Sheriff - R16, R17
County Dispatch Manager - R16
County Administrator - R1, R2, R18, R19
Board of Supervisors - R18, R19
All School Superintendents - R15

Exhibit A. Interviewees in the Investigation

Sonoma County Water Agency

- General Manager
- Disaster Planning Analyst

Sonoma County Office of Education

- Superintendent
- Deputy Superintendent
- Director, Environmental Health and Safety
- Director of Operations
- USDOE Project Director
- Loss Prevention Director – Redwood Empire Schools’ Insurance Group
- Technology Director
- Technology/Network Managers (2)
- Information Systems Manager

Large-sized School District

- Superintendent
- Deputy Superintendent
- Disaster Planning Analyst

Medium-sized School District

- Superintendent
- Supervisor of Maintenance and Operations

Small-sized School District

- Superintendent

Information Systems Department

- Director
- Division Director
- Assistant Manager – Radio and Communications
- Assistant Manager – Telephone Systems

Sheriff’s Department

- Sheriff and Coroner
- Assistant Sheriff
- Captain - Detention Division
- Captain – Patrol Bureau
- Captain – Administration Bureau
- Lieutenant (2) – Patrol Bureau
- Dispatch Manager

Exhibit B. List of documents made available to the grand jury

- Sheriff’s Organization
  - Jail Evacuation Plans
  - Dispatch Center Evacuation Plan
  - Order for TD 280 Switch – to switch County 911 lines to Santa Rosa Police Department
  - Procedure managing outside access to Sheriff’s Radio Frequency
  - Sheriff Procedure – Rules and Regulation on Conduct
  - County Dispatch Center – Disaster Response and Recovery Plan (written during this investigation)
- Sonoma County Information Services Department (ISD)
  - Sonoma County Telecommunications Network
  - County of Sonoma Radio Relay Network
  - Disaster Recovery Exercise Recap
  - Extract from Strategic plan, titled *Expanding Disaster Recovery*
- Sonoma County Office of Education
  - Trainings on Safe School Plans and School Crisis Response
  - Emergency Preparedness Plan for the main facility
  - Academic Aftershocks – a video featuring the impact of the Northridge Earthquake on California State University - Northridge
  - Practical Information for Crisis Planning – A Guide for Schools and Communities
  - Activity Summaries SCOE/USDOE Project, October 1, 2004 – March 31, 2006
  - Changes to School Safe Plan September 29, 2004
  - Community Health Profile for the Bi-County Redwood Coast Region
  - Emergency Response and Crisis Management Leadership Workshop description
  - General Safe Work Practices for all Employees
  - Earthquake Hazards Checklist
  - List of Emergency Management Activities prior to USDOE grant
  - Loss Recovery Resource Guide – Redwood Empire Schools’ Insurance Group
  - EOC/Incident Command System SEMS Organization Chart for Schools
- Sonoma County School Districts
  - Fort Ross School District Administrative Flow Chart for 2004-2005
  - Fort Ross School Safety Plan
  - Fort Ross Disaster Preparedness Plan
  - Cloverdale Unified School District Emergency Action Plan
  - Monte Rio School Emergency Action Plan
  - Petaluma City Schools Emergency Plan
  - Piner-Olivet Union and School District Emergency Closure Procedures
  - Doyle Park Comprehensive School Safety Plan 04-05
  - Post Earthquake Damage Evaluation and Reporting Procedures for California Schools
- Sonoma Tax Collector Office
  - Disaster Recovery Plan – A list of systems

Exhibit C – Basic Principles of Disaster Recovery and Business Resumption

All organizations eventually consider how best to protect their well-defined infrastructures which consist of processes, procedures, and communication mechanisms, collectively referred to as *system(s)or application(s).* The system may be manual, computer-based, or both. Normally this protection will be against disasters such as fire, earthquake or explosion. For example, manual systems have historically made use of fireproof cabinets, safes, vaults, or duplicate copies of the paperwork kept in two places. The expectation was that vital records, or *data,* could withstand the disaster, or safe copies in a safe location could be used to replenish the original data. The organization would then quickly be able to resume "business as usual," once the disaster was over. With the advent of computer-based applications the analog of fireproof cabinets etc., became necessary.

Disaster Planning

Since more elaborate schemes require more investment, it is vital that an organization carefully prioritizes the criticality of its systems and develops a *disaster plan.* The plan will usually try to identify so called *single points of failure*, identifying those pieces of equipment that should be duplicated, if possible, to reduce the probability of a disaster taking out a single critical piece of equipment.

An organization needs to determine which of its applications are critical to its ability to continue business, then decide how best to protect the critical data so that it is not lost in a disaster, or can be replaced in total or at least to an agreed to point in time. The most basic form of protection is to take periodic electronic copies of the data, typically on magnetic tape, typically nightly, and store them at a separate location. Ideally the second location is not adjacent to the primary location, or on the same earthquake fault-line! It is a form of insurance, and just as with insurance one can pay higher premiums for better coverage. An organization may decide to have multiple centers, with equipment mostly duplicated, or a second center with only enough equipment for the priority work. Until the late 90's most organizational computing was done on a single, large computer, a *mainframe.* As the personal computer (*PC*) grew in power and functionality, applications began to move to *servers,* larger PC's that could handle multiple users concurrently. Sonoma County has both a mainframe and servers, and the disaster plan for each will probably be different. For example, it is relatively easy to distribute multiple servers to multiple locations, and connect them over the network such that they can be a backup for each other. One other option for Sonoma County is to find another organization with exactly the same systems and agree to be mutual backup for each other.

Regardless of the depth of coverage in the plan, it is good practice to have "fire-drills," at least annually, to test that the organization can recover from the backup data.

Business Resumption

This refers to the process of identifying all of the steps that will be required to get back to normal after a disaster. Again, it requires senior management to identify the critical applications so that they can be restored first if there is a resource issue. Sometimes it can take many weeks to get everything back to normal. This may involve temporary labor, overtime, weekends, and cooperation from trade unions, suppliers or customers. Frequently, the business resumption plan will point to improvements that are needed for the disaster plan.

By default or by design, an organization may decide to do nothing on these two fronts. With the integration of computers into our daily work and personal lives this is most unlikely to be a prudent strategy.

EXHIBIT D Glossary of Terms in Disaster Recovery and Business Resumption

Application	A suite of computerized programs to handle a specific business requirement, e.g. Payroll
Application Code	Instructions stored in a computer that detail the precise steps that must be applied to each transaction entered
Backup	The process of copying an entity, usually a data file, to ensure there is a second copy if the primary copy is lost or destroyed
Business resumption	The process of resuming day-to-day activities once a disaster is at an end
Cluster	A grouping of servers, interconnected to each other
Disaster Plan/Management	A document detailing the steps to be taken to a) protect against a disaster's impact, and b) to recover from the disaster
Data Processing	Use of computers to process organizational data
Disaster Recovery	The detailed steps by which an organization mitigates the effect of a disaster
Distributed servers	Practice of locating servers in separate locations while still connected via a network
Full Cost Recovery	The practice of recovering all data processing costs by charging the users according to their specific usage
Hardwiring	Connecting computer and networks together in a rigid and inflexible way
Network	A telephonic or fiber cable arrangement providing interconnection between users and computer equipment
Non-stop	A computer system designed with internal redundancy to ensure that the computer system never fails (short of a physical disaster)
Packaged Application	A purchased application (rather than an internally developed unique application) providing the business function required
Redundancy	The practice of including additional equipment that is specifically backup for a similar piece of equipment
Server	Larger PC, capable of supporting many users concurrently; an alternative to individual personal computers
Single Point of Failure	A single entity in the system set up that has no identical duplicate or backup. May be computer hardware, a network controller, or even a person
Software	Instruction sequences placed in the computer system that provide a given function, for example, control of the network
System	An application or collection of Applications. Use sometimes includes the computer equipment on which the Applications reside
Third Party Supplier	Supplier of a packaged application; usually not the primary provider of the computer equipment
Transaction Processing	Applications that provide an inter-active interface that allows the user to process one transaction at a time, e.g. a bank tellers counter top terminal