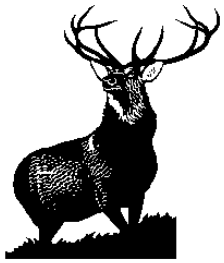

THE HARTFORD

Loss Control Department

Technical Information Paper Series

Continuity Planning for Computer Operations: *An Overview*

TIPS Series S 625.301 Printed in U.S.A.

Continuity Planning for Computer Operations: An Overview

Understanding the Need for Emergency Preparedness Planning

In a recent survey, half the risk managers surveyed reported that their organizations had experienced natural or human disasters. Were their facilities prepared for these events? Perhaps not. Despite the need, many risk managers fail to prepare adequately for emergencies. Consider these statistics:

- Fewer than 25% of American businesses have contingency plans.
- In the United States, 68% of business-affecting disasters are caused by human error; 25% by technology (hardware and software) failures; 5% by natural disasters; and 2% by intentional causes.

In terms of business survival, the results can be devastating...

- Of companies that experience a disaster but have no business recovery plan in place, 43% never reopen.
- Of 350 businesses operating in New York's World Trade Center before the 1993 bombing there, 150—that's 43%—were closed a year later.
- 70% of businesses that closed for a month or more failed to reopen, or failed altogether within three years.
- Most companies that must operate ten or more days without their computers will never fully recover.

...and the costs enormous:

- Within eight days of an extended computer outage, a company loses an estimated 2 to 3 % of its gross sales.
- 55% of organizations have experienced a disruption or inability to access computer systems for more than an hour, and 11% of large computer users report disruptions of a day or more.
- Three-quarters of businesses reach critical or total loss of functionality within two weeks of losing computer support.

Why Plan for Emergencies?

Disaster can strike at any time. Although most people think of disasters as naturally occurring events such as hurricanes or earthquakes, other events or conditions can have disastrous effects. Changes in how business is conducted can exacerbate emergency situations. The growing dependence on technology and the increasingly complex hazards of various manufacturing operations and processes increase the frequency, immediacy, and severity of disasters—both natural and technological—and contribute to the difficulty of recovery. In today's business climate, it is more important than ever to have a well-considered, comprehensive *Emergency Preparedness Plan* in place and ready to be activated.

How Can an Emergency Preparedness Plan Make a Difference?

Having an Emergency Preparedness Plan allows you to make decisions about how to proceed with emergency response and recovery *before* an emergency situation develops, when you are best able to make difficult decisions. Pre-planning allows for better prevention, better response, and better recovery. Should a disaster strike, the actions taken in the first minutes and hours can make all the difference to how soon—or *if*—normal operations can be resumed.

Without a plan, people will spend the initial precious minutes of an emergency situation frantically trying to decide what to do, who should do it, and what to tackle first. With a comprehensive plan in place, an organized, prioritized, *practiced* response can begin immediately, thus mitigating damage and perhaps even preventing loss of life.

In a recent survey, four of five risk managers reported that their plans had been effective during emergency situations. Another study showed that companies with disaster recovery plans experience an average disruption of four to six hours, whereas companies without such plans experience average disruptions of ten hours.

Although developing and implementing an effective Emergency Preparedness Plan can be costly and time-consuming, these costs are insignificant when compared to the potential losses a company must bear in the event of a major catastrophe.

What Is an Emergency Preparedness Plan?

An Emergency Preparedness Plan (or EPP) is the development, documentation, testing, evaluation, and implementation of policies, procedures, organizational structure, information, and resources that an entity can use to assess potential hazards, develop and prepare an appropriate response to each hazard, and develop and prepare strategies for recovery.

While Emergency Preparedness objectives may differ from one organization to another, they are almost always directed toward protection of people, protection of property, and preparation for the organization to resume productive operations as soon as possible.

An Emergency Preparedness Plan generally encompasses three areas:

- **Emergency Preparedness** is the process of developing and defining roles and responsibilities, procedures, and resources for the Plan.
- **Emergency Response** is the process of implementing the organization's policies, procedures, and actions to stabilize and control an emergency as it occurs and throughout its duration.
- **Emergency Recovery** is the process of implementing the organization's policies, procedures, and actions to resume the organization's normal operation.

Why Computer Operations Should Be Covered by Your Organization's Emergency Preparedness Plan

For most companies, the information created, processed, and stored using computer systems is a vital corporate asset that must be safeguarded. This recognition, along with legislation implying executive accountability for business continuity, has led to an increase in the need for disaster recovery planning for automation hardware, software, and data. The increased functionality of automation equipment, increasingly widespread computer literacy, and innovative uses such as electronic commerce on the Internet, have made automation integral to success in delivering products and services.

However, *protection* of this valuable asset is often overlooked or only nominally considered when automation projects are initiated. This lack of foresight can make it difficult to backtrack to justify the costs of developing and maintaining disaster recovery plans at a later date. By developing a business contingency *strategy*, you will provide the framework for disaster recovery plans that integrate your business and continuity planning.

Roles and Responsibilities

Management must be involved at all levels to provide commitment, input, decisions, and approval. Technical support personnel are needed to provide information on hardware, software, and data requirements; to help plan the recovery process; and to assist with testing. Depending on the size of the company, one or more staff members may be dedicated to the development of the business impact analysis, disaster recovery plans, ongoing Plan maintenance, and periodic testing.

Getting Started

Ideally, planning for any automation project will incorporate business contingency planning. Include discussion of criticality, protection, and recovery of automation hardware, software, and data in planning for any project. Include costs for protection, mitigation, and disaster recovery in the project funding.

For many organizations, though, this planning has not been done. Typically, an organization will have a long-established mix of personal computers, distributed systems, and possibly a mid-tier or mainframe computer, that is somehow interrelated and constantly changing. There may be little or no documentation of the systems available. Since the development funds have probably been exhausted, there are no ready resources for emergency planning or recovery.

If your organization is in a similar situation, you can start the emergency planning process first by defining what is critical, and then by establishing what level of risk you are willing to accept. This is accomplished by conducting a risk analysis or business impact analysis.

Business Impact Analysis

An effective business impact analysis (BIA) will establish a clear picture of the critical functions or services that are dependent on computer automation that must be restored following an emergency. Since the BIA also serves to communicate to management the potential effect of emergency situations on automated functions, it can also be used to obtain management's commitment to provide the resources needed to accomplish disaster planning, or to confirm management's acceptance of the risk of *not* planning for disaster recovery.

In a business impact analysis, you will define and prioritize critical functions of the business, establish recovery time-frame requirements, and determine the computer automation necessary to support the critical functions. Thus, you can develop specific mitigation and disaster recovery plans appropriate to support the critical function requirements.

Develop Plans Specific to Your Needs

Depending on the size and complexity of your organization, one plan may cover all of your automation processes, or you may need separate plans for special needs. Individual plans may be required for the hardware (such as a distributed system or network communications environment) and the software (such as the operating platform, application software, and data repositories). You may even need to create separate plans for types of data repositories, such as hierarchical databases or relational databases, if they are handled by specialized units.

Preparedness

Prevention and protection are the best and most economical strategies for emergency preparedness. Effective protection of automation hardware, software, and data repositories prevents disasters *and* significantly reduces the *impact* of potential disasters. For hardware, simple measures such as surge protectors, battery backups, uninterruptable power supplies (UPS), physical security, and environmental control can provide basic prevention. Make backup copies of critical software and data on a regular basis, and store them offsite, along with equipment configuration files, current recovery plans, and documentation.

More complex preparedness strategies for hardware may involve backup generators, equipment redundancy, quick-ship contracts, vendor hot sites or cold sites, mobile recovery units, and/or reciprocal agreements. Data and software protection may include disk mirroring, shadow copies, image copies, incremental backups, access security, virus protection, and/or hierarchical storage techniques. Bear in mind that the increase in the cost of preparedness is generally exponential as you approach zero tolerance for down time.

Recovery

Develop plans for the recovery of automated processes and communication networks connecting all data processing environments. These plans must clearly document the hardware, software, and data requirements. A good plan will identify assumptions, recovery location(s), recovery and management teams, notification and contact lists, response procedures, recovery processes, minimum recovery requirements, and functions or services to be recovered. Develop an ongoing process for testing and maintaining the Plan. The management of the areas or functions supported by the Plan should review and approve the Plan in order to ensure its consistency with their expectations.

References

DePompa, Barbara. "Disaster strikes! Are you ready?" *Information Week*, 527: 49-64, May 15, 1995.

Devlin, Edward S., et al. *Business Resumption Planning.* Boston, MA: Auerbach Publications, c1997.

Dunham, Ralph. "Are you ready for disaster?" *Computing Canada*, 23 (7): 32, March 31, 1997.

Effgen, K. F. "Presenting the business case for a network-based disaster recovery planning program." *Telecommunications* 26 (11): 28, 30, November 1992.

Winslow, Ron, and George Anders. "How new technology was Oxford's nemesis." *Wall Street Journal*, Col. 3, Pg. 1, Sec. B, Thursday, December 11, 1997.

Continuity Planning for Computer Operations: An Overview

Roles and Responsibilities

- ☐ Management must be involved at all levels to provide commitment, input, decisions, and approval.
- ☐ Technical support personnel will be needed to provide the hardware, software, and data requirements, to help plan the recovery process, and to assist with testing.
- ☐ One or more staff members may be dedicated to the development of the business impact analysis, disaster recovery plans, ongoing Plan maintenance, and periodic testing.

Getting Started

- ☐ define what is critical
- ☐ establish what level of risk you are willing to accept

Business Impact Analysis

An effective business impact analysis (BIA) can

- ☐ define and prioritize the critical functions or services that are dependent on computer automation that must be restored following an emergency
- ☐ establish recovery time-frame requirements
- ☐ determine the computer automation necessary to support the critical functions
- ☐ obtain management's commitment to providing the resources needed to accomplish disaster recovery, or confirm management's acceptance of the risk of *not* planning for disaster recovery.

Develop Plans Specific To Your Needs

- ☐ Determine the extent of planning needed for your organization. Depending on the size and complexity of your organization, one Plan may cover all of your automation processes. Separate Plans may be required for
  - ☐ hardware (such as a distributed system or network communications environment)
  - ☐ software (such as the operating platform, application software, and data repositories)
  - ☐ types of data repositories, such as hierarchical databases or relational databases, if they are handled by specialized units.

Preparedness

- ☐ Hardware protection measures (surge protectors, battery backups, uninterruptable power supplies [UPS], physical security, and environmental control)
- ☐ Software protection measures (make backup copies of critical software and data on a regular basis, and store them off-site, along with equipment configuration files, current recovery plans, and documentation)

Recovery

Develop plans for the recovery of automated processes and communication networks connecting all data processing environments.

- ☐ A good plan will identify:
  - ☐ assumptions
  - ☐ recovery location(s)
  - ☐ recovery and management teams
  - ☐ notification and contact lists
  - ☐ response procedures
  - ☐ recovery processes
  - ☐ minimum recovery requirements
  - ☐ functions or services to be recovered
- ☐ Develop an ongoing process for testing and maintaining the Plan.
- ☐ Request that management of the areas or functions supported by the Plan review and approve the Plan, in order to ensure its consistency with their expectations.

General Emergency Instructions

- ☐ Develop policies and procedures for all potential disaster scenarios, especially those that are likely to occur frequently, or those that could have a severe impact, such as:
  - ☐ heating, air conditioning, or power outage
  - ☐ medical emergency
  - ☐ communication line failure
  - ☐ hurricane, tornado, flood, earthquake, snow or ice storm
  - ☐ civil disorder, computer hacker, or bomb threat
  - ☐ fire or smoke emergency
  - ☐ water main break, sprinkler leakage, or sewage backup
- ☐ Create a contingency plan for "mutual aid" assistance from other companies or vendors.
- ☐ Formalize and stage practice exercises.
- ☐ Formalize a 24-hour emergency line of credit, for immediate access.

Continuity Planning for Computer Operations: Software and Network Protection

Inventory Controls

- ☐ Maintain a current inventory of all hardware and upgrades.
- ☐ Create a master log of DIP switch and jumper settings.
- ☐ Create a master log of miscellaneous cables, gateways, wire frames, and other equipment.
- ☐ Maintain a current inventory of all software and upgrades.
- ☐ Create a master log of software service packs, fixes, and order of installation.
- ☐ Log the configuration settings used for the installation of hardware and software.
- ☐ Store warranties, manuals, installation booklets, and other paperwork away from computer.
- ☐ Store original copies of software and upgrades away from computer.

Saving and Restoring Documents

- ☐ Make a copy first, then store originals and use the copy.
- ☐ Obtain as much RAM as you can afford on clients and servers.
- ☐ Enable "full auto saves" versus "fast saves," for easier restorations.
- ☐ Enable "make back-up copy" whenever offered, to protect originals.
- ☐ Name and save documents immediately, to place working document into hard disk space.
- ☐ Re-save documents often, especially after many revisions.
- ☐ Copy documents onto sets of "copied" diskettes. If one fails, there is a second copy.
- ☐ Make regular "mini" backups of "my documents" or similar files.
- ☐ Use removable diskettes (e.g., ZIP, Jazz, TR tapes) for mini backups.
- ☐ Rotate mini backup media, and replace media at 80 percent use level.

Software And Data Duplication

- ☐ Use automated software to conduct daily incremental backups.
- ☐ Use automated software to conduct weekly full backups to be sure that all resources are covered.
- ☐ Rotate backups through a set cycle.
- ☐ Maintain at least three copies in rotation, with at least one copy stored off-site.
- ☐ Replace backup media at 80 percent recommended use, to avoid bad sectors, etc.

Storage of Software and Data Backup

- ☐ Place backups in U.L.-listed records containers.
- ☐ Store containers off-site at a location that is accessible 24 hours a day, 7 days a week.
- ☐ Ensure that off-site storage is environmentally conditioned and secured, allowing only authorized access.
- ☐ Ensure that off-site storage is far enough away so that it will not be affected by an area-wide disaster that may involve the company location.
- ☐ Clearly mark containers that have critical backups and documentation (e.g., use red containers).
- ☐ Rotate off-site backups.
- ☐ Use off-site backups when performing disaster recovery exercises.

Virus Protection

- ☐ Install virus protection software for network servers.
- ☐ Install virus protection software for client computers.
- ☐ Run background checking portion of virus software at all times.
- ☐ Automatically scan all disks, removal disks, and tapes at least weekly, (preferably nightly).
- ☐ Automatically scan all client computer hard disks at least weekly (preferably daily at logon).
- ☐ Automatically update virus protection software at least monthly.
- ☐ Scan all diskettes, removable media, CDs, and DVDs before use.
- ☐ Before using input from the Internet or electronic mail, load it to diskette and scan.
- ☐ Develop procedures for handling viruses, in order to limit their impact should they enter the system.

Software and Hardware Compatibles

- ☐ Develop software and hardware certification procedures.
- ☐ Always pre-test new software and hardware on non- critical PCs.
- ☐ Test, re-test, and test again, until there are no apparent conflicts.
- ☐ Develop a contingency fall-back plan *before* installation of changes to critical systems.
- ☐ Be ready for client and server “crashes," and have backup drives ready “online.”

Internets, PPTP and VPNs

- ☐ Use encryption on Point to Point Transfer Protocols (PPTP) when using any ISP (Internet Service Provider) to connect to Virtual Private Networks (VPN).
- ☐ Use firewall and proxy servers to insulate your network from the Internet.

- ☐ Use encryption on E-mail, documents, teleconferencing, and Internet phone, when working with sensitive data.
- ☐ Block, or severely restrict access to, files, modems, printers, and faxes from Internet users.
- ☐ Use "Caller ID" services to identify hackers and password-cracker programs.
- ☐ Lock out hackers and password-cracker programs after three attempts.
- ☐ Change passwords at least quarterly, and require new passwords of 8 to 64 alphanumeric characters.
- ☐ Use private and public key encryption services whenever possible.

Intranets, LANS, and WANS

- ☐ Carefully control access to software, data files, printers, modems, and faxes within an Intranet.
- ☐ Change passwords at least quarterly, and require new passwords of 8 to 64 alphanumeric characters.
- ☐ Set company-wide system and user policies, and update them daily.
- ☐ Disable access by temporary or terminated employees, vendors, and customers.
- ☐ Lock down desktop software installation whenever possible.
- ☐ Create "read only" folders on Intranets.

Continuity Planning for Computer Operations: Hardware Protection

Hard Drive Maintenance and Upkeep

- ☐ Always make a full backup before performing hard drive maintenance.
- ☐ Clean out temporary files regularly.
- ☐ Clean out the "trash can" or "recycle" bin at least weekly.
- ☐ Clean out "trash cans" or "deleted items" folders in electronic mail programs.
- ☐ Archive and clean out calendar information at least twice per year.
- ☐ Run compression utilities for various programs that use "data bases," at least weekly.
- ☐ Run basic "scan disk" (or similar software) at least weekly on all machines, or at startup.
- ☐ Run thorough "scan disk" (or similar software) at least twice a year to mark defective sectors.
- ☐ Run a hard disk defragmentation program at least monthly, to increase computer efficiency.

Hardware Duplication

- ☐ Contract for hot site, warm site, cold site, or mobile unit vendor services.
- ☐ Contract with hardware vendors for quick shipment of critical equipment.
- ☐ Check software contracts/licenses for clauses pertaining to use at alternate location during emergencies.
- ☐ Create a contingency plan for the purchase, installation, and certification of replacement equipment.
- ☐ Determine the excess cost associated with "Rush" manufacturing, installation, and certification.

Duplicate Servers

- ☐ Determine the cost of purchasing and installing a true duplicate server.
- ☐ Determine the cost of upgrading the "back-up" server to full server.
- ☐ Determine the cost of duplicate software, including license fees for multiple users and sites.
- ☐ Determine the cost to maintain "exact" duplicate servers, including all overhead expenses.
- ☐ Locate servers in separate areas, fire divisions, or buildings.

Continuity Planning for Computer Operations: Facilities, Environmental Controls, and Security

Main and Emergency Power

- ☐ Ensure that power panels are fed from separate trunk lines.
- ☐ Ensure that power panels are easily accessible.
- ☐ Ensure that power to critical equipment is distributed from separate power panels.
- ☐ Verify that circuit breakers are clearly marked and up to date for all attached equipment.
- ☐ Ensure that panels, circuit breakers, and UPS rating exceed the total wattage of all attached equipment.
- ☐ Ensure that panels, circuit breakers, and UPS rating exceed the total volt-ampere rating of all attached equipment.
- ☐ Maintain line-to-line steady state voltage at +10% to -8% of the normal rated voltage.
- ☐ Verify that all critical communication equipment is protected by noise-shielded and surge-protection devices.
- ☐ Verify that all critical equipment is powered by an Uninterruptable Power Supply (UPS).
- ☐ Ensure that the UPS is "network aware" and capable of starting the shutdown process.
- ☐ Ensure that the UPS is fed from filtered surge-protected power units.
- ☐ Use backup emergency generators for "No Down Time" applications.
- ☐ Ensure that emergency systems shut-down procedures are documented; include procedures for an ordered systems shut-down.
- ☐ Ensure that emergency room power down is available in the room and at a remote location.

Environmental Controls

- ☐ Maintain computer room air temperatures at 72^{o} F, with a variance of no more than +/- 2^{o} F.
- ☐ Maintain computer room humidity at 50%, with a variance of no more than +/- 10%.
- ☐ Ensure that computer fans have unrestricted intake of cool room air.
- ☐ Maintain media storage in conditions with similar temperature and humidity as the computer room.
- ☐ Allow transported media to adjust to computer room conditions before use.
- ☐ Conduct regular housekeeping and dusting.
- ☐ Professionally clean inside ductwork and under raised floors periodically.
- ☐ Use HEPA filters in vacuums, to limit re-circulation of dust.

- ☐ Use dust covers to protect unused and powered down printers, faxes, scanners, and keyboards.

Detection and Suppression Systems

- ☐ Ensure that fixed fire detection, alarm, and fire suppression systems are installed and maintained according to local and National Fire Protection Association (NFPA) codes, OSHA requirements, and manufacturers' specifications.
- ☐ Install wet or pre-action sprinkler systems in all areas.
- ☐ Install fire alarm signals in all areas.
- ☐ Verify that fire alarm systems transmit signals to a 24-hour monitoring station.
- ☐ Install smoke detectors below the raised floors, on ceilings, and above suspended ceilings.
- ☐ Install a water detection system if flooding is a potential hazard under raised floors.
- ☐ Test all detection, alarms, and suppression equipment on a regular basis.
- ☐ Place CO_2 U.L.-listed fire extinguishers near computers.
- ☐ Provide regular training in the use of fire extinguishers to employees.
- ☐ Install illuminated exit signs and post evacuation routes in all areas.
- ☐ Practice evacuation drills regularly.
- ☐ Post the emergency number on all phones (i.e., "9-911" or "911").
- ☐ Provide a floor panel lifter for immediate access to the area under raised floors.
- ☐ Provide water-tight salvage covers.

Security Controls

- ☐ Limit access to computer areas (use ID cards, key pads, door locks, and guard stations).
- ☐ Limit access to computer systems (use BIOS passwords, client and network passwords).
- ☐ Secure and limit access to location of keys, passwords, combination lock numbers, etc.
- ☐ Install burglary/intrusion alarm systems, closed-circuit TV monitoring, guard services, and sign-in and sign-out sheets.
- ☐ Use "power on" locks on computers.
- ☐ Keep computers, especially laptop equipment, out of sight; lock computers on or in desks, cabinets, or in a storage room.
- ☐ Change combinations and passwords quarterly, or when personnel changes occur.