INFORMATION TECHNOLOGY CONTINGENCY PLANNING

Randy Harris
Air Force Institute of Technology

Michael Grimalia
Center for Cyberspace Research
Air Force Institute of Technology
Michael.Grimaila@afit.edu

ABSTRACT

Natural disasters, terrorist acts, large-scale accidents, and cyber attacks all have the potential to cause a catastrophic loss of information technology systems and infrastructure. In the event of such an outage, it is vital for organizations to ensure their business processes which are vital to the mission and survival of the organization, continue. No matter what contingency planning process is used, the ultimate success of a contingency recover depends on the personnel implementing those plans and procedures. In this paper, we examine existing guidance on contingency planning, review the contingency planning process, and highlight the importance of individuals in assuring the success of contingency operations.

Keywords

IT contingency planning, disaster recovery, information security

INTRODUCTION

In today's world of terrorism, climate change, and an ever-increasing reliance upon Information technology (IT), an IT contingency plan is a virtual requirement for any organization. The time and money invested in developing and writing an IT contingency plan can pay enormous dividends in the event of a major disaster. While a plan is good, it must be tested, revised as necessary, and the people who use it must be trained. Perhaps one of the most important assets a company has during a contingency is dedicated personnel who can solve problems not covered by the IT contingency plan.

Utilizing this or another IT contingency planning process will enable organizations to maintain critical IT systems and business processes during a crisis. No matter what contingency planning process is used, the ultimate success of a contingency recover depends on the personnel implementing those plans and procedures. The ability of dedicated organizational personnel to overcome personal loss for the good of the organization and customers is one key to success. In addition, personnel with the ability to develop solutions to problems no one anticipated are extremely valuable during a contingency situation. The combination of a comprehensive and tested contingency plan with these types of personnel will enhance an organization's recovery capability.

CONTINGENCY PLANNING DEFINED

The National Institute of Standards and Technology states that, "IT contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption" (Swanson et al., 2002). In addition, IT contingency planning should be part of a larger organization-wide contingency plan. Sauter and Carafano offered this definition of organizational contingency planning:

> *"A contingency plan is a comprehensive statement of actions to be taken before, during, and after a disaster. A successful planning process must achieve three goals: (1) create awareness of potential disasters, (2) define actions and activities that will minimize disruptions of critical functions, and (3) develop the capability to reestablish business operations."* (Sauter & Carafano, 2005)

A properly designed, written, and tested IT contingency plan incorporated into an overall contingency plan should help any organization withstand and recover from a disaster.

Threats

There are many potential threats that can cause a disaster serious enough to require an organization to implement its IT contingency plan. Natural phenomena, such as earthquakes, hurricanes, and tornadoes, have the potential to cause a catastrophic outage of IT systems. Recent events such as Hurricane Katrina, the tsunami in Asia, and the forest fires in southern California all testify to the devastating and destructive nature of natural phenomena. Almost assuredly, IT systems in buildings at these locations were not spared when these phenomena destroyed everything in their path.

In addition, there are also human-caused catastrophic events that require contingency response. These events can be intentional or unintentional. Unintentional human-caused events include things such as physical accidents, ignoring safety procedures, and mistakes entering programming code. Intentional events are often the work of disgruntled employees, thrill seekers, or terrorists.

Janczewski and Collarik assert that terrorist activities affect an organization's IT systems in three primary ways. Two ways applicable to this discussion are a "Direct attack on IT facilities" or "Collateral IT damages resulting from terrorist attacks against other targets" (Janczewski & Colarik, 2005). An example of a non-intentional human caused failure is found in the case of Pilot Network Services Company. Bernato explains:

> *"ON APRIL 25, PILOT NETWORK SERVICES went out of business, abandoning 200 customers that relied on them for something rather important: security…. Yet this was not some high-flying dotcom that appeared one day, took some easy venture capital, then vanished. Pilot was an established, 8-year-old vendor with 400 employees and, by most accounts, superior security technology and practices. Its customers included PeopleSoft, VisionTek, The Washington Post Co. and several large health-care institutions and banks."* (Berinato, 2001)

Although, Pilot Network Services did not go out of business on purpose, the impact was catastrophic to the companies they supported. In light of the many catastrophic events that require a contingency response, the value of a contingency plan is great.

Contingency Plan Value

The value of an IT contingency plan may seem obvious, but in case there is doubt, hare are a few examples. First, Janczewski and Colarik note that:

> *"A decade ago, a large earthquake shook Kyoto, Japan. Significant parts of the downtown were totally destroyed. It is estimated at that time that about 20% of businesses did not survive the quake due to the destruction of their computer-located records. On the other hand, we read a report on actions taken by management of a major U.S. West Coast bank whose headquarters was destroyed by a fire. Within a day they were able to resume basic operations, and within a week resume all regular activities. This was made possible because management had prepared a solid business continuity management program."* (Janczewski & Colarik, 2005)

In addition, there can be large monetary sums at stake. Sauter and Carafano when speaking about the impacts of a major outage:

> *"For Example, according to a 1998 survey by Strategic Research Corporation, the financial impact of a major outage would have a significant impact on America's largest companies including costing brokerage operations $6.5 million per hour. A breakdown in the credit card sales authorization system would cost $2.6 million per hour…. The effects of disaster are perhaps the most significant on small businesses. Data collected by FEMA suggest that half the small companies that experience a disaster go out of business within two years."* (Sauter & Carafano, 2005)

It can be assumed that these figures have risen appreciably over the last decade. With so much at stake, it seems as if every organization would have an IT contingency plan, but this is not the case. In fact, only 75 percent of medium and large companies have contingency plans, and of those, only one in four has tested them in the last half a decade (Sauter & Carafano, 2005). These figures seem strange when there are resources available to assist organizations to build an IT contingency plan. One of theses resources is the National Institute of Standards and Technology's (NIST) and their seven-step contingency process.

CONTINGENCY PLANNING PROCESS

The NIST recognizes that assisting organizations with contingency preparedness is advantages for the US as a whole. Logically, the better prepared both private and governmental organizations are to face contingencies the less impact these events will have on the economy and security of the US. The NIST provides the following seven-step contingency planning process as shown in Figure 1 (Swanson et al., 2002):

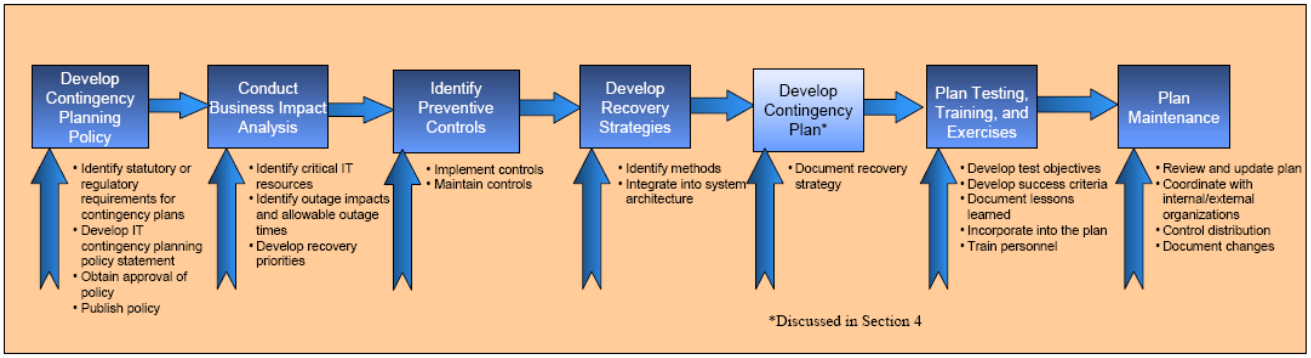

Figure 1. Contingency Planning Process (Swanson et al., 2002)

Step 1. Develop the Contingency Planning Policy Statement

This is perhaps the most difficult part of the process because to begin this step the organization must realize that the contingency planning process is necessary. Philpot states that the first big challenge is to "reach an agreement that something needs to be done" (Philpott, 2007). Until personnel, especially senior management can be convinced contingency planning is important, this first step will never begin. Once the need is established, the policy statement writing can begin. The NIST offers that, "The contingency planning policy statement should define the agency's overall contingency objectives and establish the organizational framework and responsibilities for IT contingency planning." Wrobel suggests the following objectives or overriding themes for the Policy Statement, referred to by Wrobel as an "Administrative Statement":

1. Protect Human Life
2. Minimize Loss and Risk to the Company
3. Maximize Ability to Recover
4. Protect the Company From Lawsuits
5. Maintain Competitive Position
6. Preserve Customer Confidence and Goodwill
7. Define What is at Stake
8. Overview of Preliminary Business Impact Analysis
9. Synopsis of Recovery Strategy

By considering these objectives, the organization building an IT contingency plan will capture the requirements that will form the bedrock of a strong plan.

Step 2: Conduct Business Impact Analysis

This step is critical to establishing what systems are the most important for the organization. The purpose of the business impact analysis (BIA) is to identify processes critical for business, or organizational success, and then marry them to the IT processes and systems that support those business processes. In addition, the BIA strives to identify the costs of losing the identified processes. The costs can be in monetary terms, threats to security and safety, or in the case of the military could be in terms of mission failure. After these steps are accomplished, system and process restoral priorities can be established (Swanson et al., 2002).

Step 3: Identify Preventative Controls

Arguably, the best way to address system outages is before they occur by utilizing preventative controls. Preventative controls should be the first course of action as long as the costs of the controls do not exceed the criticality of the system (Swanson et al., 2002). For example, a constant watch of thirty security forces guarding a state-side UASAF network operations and security center (NOSC) would help mitigate physical threats to the facility, but at likely too high of a manpower cost for the asset and likely risk. Sauter and Carafano describe four general types of "preparedness measures" that also hold true for IT contingency preparedness.

> *"There are four types of preparedness measures that might be undertaken to reduce the risk of a disaster. Deterrent measures reduce the likelihood of a disaster or deliberate attack. Preventative measures protect vulnerabilities and make an attack unsuccessful or reduce its impact. Corrective measures reduce the effect of an attack. Detective measures discover attacks and trigger preventative or corrective controls. These measures may require new practices, personnel, or equipment."* (Sauter & Carafano, 2005)

As noted above the IT practitioner developing preventative controls should be ready to look at new ways and means of protecting critical IT assets. If preventative controls fail, then recover strategies must be ready.

Step 4: Develop recovery strategies

In the event preventative controls are not successful in stopping a catastrophic outage, recovery strategies must be in place to provide continuity of the critical business processes identified during the BIA. There are a number of recovery strategies available to organization, ranging from options within and outside of the organization. As with preventative controls, the recovery strategies should focus on the priorities identified during the BIA (Swanson et al., 2002). The NIST provides the following general guidance on recovery strategies:

> *"Specific recovery methods…should be considered and may include commercial contracts with cold, warm, or hot site vendors, mobile sites, mirrored sites, reciprocal agreements with internal or external organizations, and service level agreements (SLAs) with the equipment vendors. In addition, technologies such as Redundant Arrays of Independent Disks (RAID), automatic fail-over, uninterruptible power supply (UPS), and mirrored systems should be considered when developing a system recovery strategy."* (Swanson et al., 2002)

An example of utilizing an alternate site occurred when Entergy, an electricity and natural gas provider based in New Orleans, relocated operations to their disaster recovery site in Little Rock, AR during Hurricane Katrina. Stephanie Overby notes, "Entergy's most critical applications were successfully brought online in Little Rock from backup tapes…" (Overby, 2005). Entergy's recovery strategy worked and ensured critical business processes continuity. The Entergy example provides a lesson that IT contingency planning and recovery strategies can work. The recovery strategies an organization chooses will be dependent upon the business process needs, internal capabilities and resources, and the number and type of critical systems supporting business processes.

Step 5: IT Contingency Plan Development

Perhaps the most critical step of the contingency planning process is the plan development step. The work that has gone on before this step will be time wasted unless the information is documented in the IT contingency plan. NIST's IT Contingency Plan format provides an excellent starting point for plan development (Swanson et al., 2002). However, it should not be construed to be all-encompassing and so each organization must adjust the format to meet its unique requirements. NIST describes the components of the contingency planning document below:

> *"…this guide identifies five main components of the contingency plan. The Supporting Information and Plan Appendices components provide essential information to ensure a comprehensive plan. The Notification/Activation, Recovery, and Reconstitution Phases address specific actions that the organization should take following a system disruption or emergency."* (Swanson et al., 2002)

NIST's IT Contingency Plan Format denotes the details each section and should be consulted for additional information. Finally, as confirmed by Sauter and Carafano, "Once completed, the plans" (business contingency plans, of which the IT contingency plan is part) "should be approved by management" (Sauter & Carafano, 2005). The approval of management will be much easier to obtain if, as noted earlier, management buy-in was acquired at the start of the planning process.

Step 6: Plan Testing, Training, and Exercises

The IT contingency plan must work when needed; finding out that it does not work during an emergency is much too late. Plan testing, training, and exercises will help to establish the viability of the organizations IT contingency plan. Plan testing will discover holes in the plan that must be fixed, or identify procedures that seem simple on paper, but are complex in execution. Training ensures that contingency operations personnel will understand what they must do during a crisis. Finally, exercises help ensure the effectiveness of the plan (Swanson et al., 2002).

Entergy learned the value of a well-tested contingency plan during Hurricane Katrina and its aftermath. With its headquarters in New Orleans and its primary data center located across the river in Gretna, Louisiana, Entergy had to enact their contingency plan to avert disaster. The plan, tested once each year, worked well. Operations moved to their disaster

recovery site in Little Rock, Arkansas and critical systems were online and working. Although the electricity and generators at the Gretna data center failed, which had never happened during previous tests or actual hurricanes, operations continued at the disaster recovery site (Overby, 2005). Entergy CIO, Ray Johnson, stated that, ""This is not a unique event for us," explains Johnson, "I wish it was. But we've got our disaster plan nailed. We review it at least once a year and either we conduct a drill or get to test it when a hurricane threatens us and then misses" (Overby, 2005). Mitts notes that there are many methods available for testing a contingency plan. Although the time needed, the criticality of the resources, and the funds required to perform the test will help to determine the type of test, Mitts recommends each of the following major tests be part of a testing program (Mitts, 2007):

- Drills: typically targeted at a specific response.
- Walk-Through Test
- Orientation Walk Through: a tabletop exercise that addresses all parts of the plan to orient contingency team members
- Tabletop Walk-Through: exercises all or part of the contingency plan as proposed in the test plan.
- Live Walk-Through: the contingency plan is executed as if a real contingency has taken place
- Parallel Test: Operational test is held in parallel with the actual process of critical systems to ensure systems will run correctly at the alternative site.
- Simulation Test: Scenario based test in which the participants will only have access to materials in the offsite storage to conduct their activities in the simulated recovery.
- Full Interruption Test: A live test. Potentially dangerous because it involves shutting down normal processing.

Proper training and plan testing/exercises will hone both the organization's people and IT contingency plan to a sharpness that will increase the chances of a successful disaster recovery.

Step 7: Plan Maintenance

The only thing that might be worse than no IT contingency plan, is an IT contingency plan that has become outdated. It is conceivable that a procedure that is no longer valid is more dangerous than no procedure, because during times of crisis a person under stress may not realize the procedure is incorrect and use it anyway. Unfortunately, NIST does not have a section within their IT contingency plan format for plan maintenance, only one "Record of Changes" page (Swanson et al., 2002). Wrobel recommends that contingency plan maintenance be part of the actual contingency plan (Wrobel, 1993). He suggests a "Testing and Maintenance of the Plan" section within the plan. In the event of a crisis, a current and accurate IT contingency plan should provide the best tool to ensure an organization survives.

The Human Factor

A common theme throughout much of the literature is the importance of the people who execute a contingency plan. People's ability to sacrifice their personal needs and discover solutions to new problems were key during the events of Hurricane Katrina. Stephanie Overby provides this statement from Ray Johnson, of Entergy, that provides a poignant example of employee dedication:

> *"What's unique about this story is the fact that so many people involved with the core restoration that relocated her to Jackson were on the job working hard even though they knew they had no home to return to, "Johnson says, including a senior member of the business continuity team. "People up to senior management level couldn't get in touch with family members. And these people were working twenty hours a day. It was a testament to their dedication."*

Another employee came through for Mississippi Power during the Hurricane Katrina emergency. Rufus Smith was responsible for supplying gas for the 5,000 vehicles, 14,000 gallons a day, involved in their recover effort (Cauchon, 2005). Unfortunately, there was a problem. Gas was in short supply and there was no way to purchase it and so, as Cauchon reported in USA Today,

> *"With the cash economy in shambles, Mississippi Power reverted to the barter system: electricity for fuel. It restored power to a Chevron refinery in Pascagoula and a pipeline in Collins, Miss., in exchange for a steady supply of fuel."*

These examples relate to a theory called "Societal Resilience" or "the ability to 'bounce back' after suffering a damaging blow" as presented by Boin and McConnell (Boin & McConnell, 2007). Boin and McConnell maintain that, "The research

on large-scale natural disasters strongly suggests that an effective response during the immediate aftermath (the first hours and days) critically depends on the resilience of citizens, first-line responders, and operational commanders" (Boin & McConnell, 2007). Although speaking of a society during a natural disaster, "citizens, first-responders, and commanders" within an organization also exist. Organizational members, technicians, and supervisors are a parallel to the individuals mentioned by Boin and McConnell. As such, the examples from Hurricane Katrina indicate that what could be called "Organizational Resilience" was a factor in the successful contingency efforts of Mississippi Power and Entergy Inc. It would seem the ability to "bounce back" allowed personnel to work in extreme conditions and develop new solutions to problems, while overcoming their personal tragedy.

CONCLUSION

In today's world of terrorism, climate change, and an ever-increasing reliance upon Information Technology, an IT contingency plan is a virtual requirement for any organization. The time and money invested in developing and writing an IT contingency plan can pay enormous dividends in the event of a major disaster. While a plan is good, it must be tested, revised as necessary, and the people who use it must be trained. Perhaps one of the most important assets a company has during a contingency is dedicated personnel who can solve problems not covered by the IT contingency plan.

DISCLAIMER

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

REFERENCES

1. Berinato, S, "Outsourcing: What you can do if your security vendor fails," [Electronic version]. CIO, 2001, http://www.cio.com/article/30411/Outsourcing_What_You_Can_Do_If_Your_Security_Vendor_Fails
2. Boin, A., & McConnell, A., "Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience," Journal of Contingencies and Crisis Management, 15(1), 50-59, 2007.
3. Cauchon, D., "The little company that could ," [Electronic version]. USA Today, Money October 10, 2005 http://www.usatoday.com/money/companies/management/2005-10-09-mississippi-power-usat_x.htm
4. Janczewski, L. J., & Colarik, A. M., "Managerial guide for handling cyber-terrorism and information warfare," Hershey, PA: Idea Group Publishing, 2005.
5. Overby, S., "Power up," [Electronic version]. CIO, Retrieved October 11, 2005 http://www.cio.com.au/index.php/id;515538275; pp. 1, 2005.
6. Mitts, J. S., "Business Continuity and Disaster Recovery Plans: How and When to Test Them," EDPACS, 33(5), 2007.
7. Philpott, D., "Emergency Preparedness Communications," Homeland Defense Journal, 5(6), 44, 2007.
8. Sauter, M. A., & Carafano, J. J., "Homeland Security : A complete guide to understanding, preventing, and surviving terrorism," New York: McGraw-Hill, 2005.
9. Swanson, M., Wohl, A., Pope, L., Grance, T., Hash, J., & Thomas, R., "NIST special publication 800-34 Contingency Planning Guide for information Technology Systems," Recommendations of the National Institute of Standards and Technology. Washington DC: U.S. GOVERNMENT PRINTING OFFICE, 2002.
10. Wrobel, L. A. (Ed.), "Writing disaster recovery plans for telecommunications neworks and LANs," MA: ARTECH House, INC, 1993.