ITM Whitepaper

ILLINOIS INSTITUTE OF TECHNOLOGY | *School of Applied Technology*

...because knowledge is power.

Contingency Planning for Information Technology

Joseph Carbon and Julian Hays
Edited by Ray Trygstad

12/22/09

www.itm.iit.edu

An Information Technology and Management Whitepaper from
Illinois Institute of Technology's School of Applied Technology

ITM Whitepaper: *Contingency Planning for Information Technology*

Since the beginning of time, the Earth has endured many natural disasters. From hurricanes, to volcanic eruptions, the fury of Mother Nature can be seen by just turning on the nightly news. Sometimes these events have the potential of creating more damage then just to a faraway landscape. Sometimes these disasters will happen around civilizations, creating turmoil and interruptions for all affected. These disasters can damage buildings, roads, dams, even people; however not many people stop to think that these disasters can hurt information as well. Furthermore, not many people plan for such events to occur. Without having contingency planning to deal with catastrophe, a company can be as in the dark as a person trying to find the exit in a smoke filled room.

"Their restore procedures called for the first tape to be loaded in the tape drive. Which was the first tape? Liz knew the backup procedures instructed the third shift operators to document the starting and ending tape numbers. Where was the log? Back at the office maybe…".[1] This is not a life threatening situation that Liz has been put in; this is an IT disaster recovery drill. If people are the life blood of an organization, information is the nerve impulses that allow it to function. Every day employees are transmitting purchase orders, account numbers and passwords, employee files, recommendations, product sheets, advertisements, etc… Most people now have the knowledge that the majority of this information is stored on a data server somewhere, either on the company premises or outsourced to a data warehouse. But what happens if the users suddenly lose access to this information due to some type of disaster? On top of the chaos of people becoming unplugged from the world, in much of today's business world nothing could be accomplished. To clarify a disaster, one must understand that a disaster is not just an act of nature that disrupts the earth in extreme forms; a disaster can be as simple as a computer bug that gives a hacker access to the company server or a virus installed from an e-mail.

In today's world, most businesses require their systems to be fully operational at all times in order to maintain productivity. In the event of a disaster, interruptions to core business technology services can be very costly or even fatal to the firm. Through planning and practice, an IT department can ensure that they are ready to handle these issues quickly and effectively. There are many different types of disasters that can affect informaitn technology systems with different solutions for each. Planning the solutions—and testing the planning—are key to limiting damage and loss to the company.

First, a Disaster Recovery Plan should be created, tested and maintained. In addition to this, a Business Continuity Plan should be created. These plans help ensure that in the event of a disaster, technology systems will be operational and/or accessible from a temporary location if needed. A company that already has these plans created will be able to handle a disaster much more effectively that a company that does not. There are many types of threats or disasters that could affect IT systems. It is important to identify these different threats, because they all require different planning. Natural disasters, such as storms, floods, hurricanes, tornadoes, and earthquakes can greatly disrupt IT systems. Natural disasters can occur with or without warning. In 2007, a report was published by AT&T regarding the preparedness of IT businesses in 10 major U.S. cities for natural disasters. In Atlanta, 28% of surveyed business said they had no plan in place. Atlanta ranked 6th out of the 10 major cities. This means that there are other major cities where possibly more than 30% of businesses do not have a plan for dealing with natural disasters[2]. Another threat is the failure or malfunction of both hardware and software. This threat can be lessened by

1 Hiatt, C. J. (1999). *A Primer for Disaster Recovery Planning in an IT Environment.* Hearsey: Igi Global.

2 "Natural Disaster Preparedness Survey Spurs Scary Results For Atlanta." Retrieved October 29, 2009, from http://securitysolutions.com/news/natural-disaster-preparedness/

regular software updates, maintenance, and replacement of old hardware, but planning for a major failure would be beneficial. Theft is also a high level threat, especially as more employees are using mobile devices for their work. Businesses can help by educating their employees regarding what data is safe to keep on mobile devices and what is not. It is estimated that 70% of the total U.S. workforce will be considered mobile workers in 2009. Thus, it is vital that companies invest in theft recovery and remote data deletion services for their mobile devices (Chisholm). There are also malicious attacks to plan for, such as software attacks including viruses, trojans, worms, and DDoS, or physical attacks such as acts of terror. Malicious software attacks can be defended by firewalls and anti-virus software, but having a plan to deal with a successful attack is still necessary. For any type of disaster, having a plan is key in order to "Restore normal modes of operation with minimum cost and disruption to normal business activities..."[3].

To conduct contingency planning properly, an enterprise needs to organize an provide plans for several teams: Incident Recovery, Disaster Recovery, and Business Continuity. The first planning step is to identify all critical functions and resources of the business. Then, prepare a list of all potential disasters, threats, or issues that could face these functions and/or resources. With this information, the contingency planning team can prepare a Business Impact Analysis (BIA). The BIA provides detailed information regarding the scenarios of all types of disasters or attacks. By ranking the likelihood of occurrence as well as the expected impact, the team can decide specifically what to plan for. Planning should reflect protecting or restoring the critical business functions and resources. The Disaster Recovery Team should document everything in a Disaster Recovery (DR) 'bible'."The DR bible is a reference book in which you compile all the information necessary to put a recovery plan in place."[4]. This documentation should also include contact information for all necessary personnel, as well as contact information for important vendors or service providers. Process documentation is also very important. The DR bible should include simple instructions for all regular and necessary processes, so that in the event of a missing critical staff member, or new employee, there are instructions to follow. Simply creating a recovery plan is not enough—it must be both tested and updated regularly.

"A 2007 eWeek survey of more than 500 senior IT professionals revealed that a whopping 89% of companies test their disaster recovery/failover systems only once per year or not at all."[5] In the event of a disaster, it is the job of the Incident Recovery team to get the recovery efforts in motion. An Incident Response team is responsible for assessing the incident and deciding whether or not to classify the incident as a disaster. If it is a disaster, the Incident Response team must begin the calling tree to notify all critical personnel and begin following the pre-written plans.

In addition to recovery planning, Business Continuity Planning is essential to keeping a business active and effective even in the event of a disaster. There are multiple aspects to continuity planning, both preventive and reactive. One of the simplest, yet most important preventive methods is to back up everything. It is also important to ensure that the backups are either performed at an external site, or are regularly moved to an external site. This way, in the event of a natural disaster or fire, the valuable company data is safely

3 Trygstad, R.(2009, October 8). *ITM 478-578 Lecture 07.* ITM-478/578, Daniel F. and Ada L. Rice Campus, Illinois Institute of Technology, Wheaton, IL.

4 Biddinger, N. "The Information Technology Role in Disaster Recovery and Business Continuity" | Operations > Business Continuity from AllBusiness.com. Retrieved October 29, 2009, from http://www.allbusiness.com/company-activities-management/operations/6602879-1.html

5 Chisholm, P. "Ten Tips for Successful IT Disaster Recovery Planning." Retrieved October 25, 2009, from www.infosectoday.com/Articles/DRPlanning.htm

stored in another location. While the Disaster Recovery team's focus is on reestablishing normal operations at the primary business location, it is the job of the Business Continuity Team to establish temporary operations, possibly at an external site, to ensure continued business operation during disaster recovery. In some cases, it may be most effective to outsource data backup as well as set up a secondary infrastructure. Some companies offer mobile hot-sites that can be rented and used as a temporary business site while the primary site is being restored. The use of a cloud computing service is useful to keep data constantly backed up in an external location. Purchasing Software as a Service package (SaaS) is also an excellent method of making applications and resources accessible while using another company's infrastructure. The Green Bay Packers football organization recently began a partnership with a company called Venyu, who "offers enterprise software via software as a service (SaaS) solutions for data protection, availability and disaster recovery". Additionally, the Green Bay organization purchased online data backup and recovery solutions from a company called AmeriVault[6]. Between temporary rental services and full outsourcing solutions, a Business Continuity team should come up with a plan that will provide the company with sufficient services during the primary site's disaster recovery down time.

Let's look at a couple of stories that that illustrate why contingency planning is a key to IT continuity of operations and may even avert disaster.

In 1983, World War III almost began between the Soviet Union and the United States when new Soviet software "displayed" five ballistic missiles coming from the United States towards the Soviet Union. Fortunately, Soviet Lieutenant Colonel Stanislav Petrov had figured there must be some sort of glitch because America surely would not send only five missiles in the face of total annihilation[7]. Sure enough, the Colonel's trust was rewarded when it was determined that a software bug mistook something else for U.S. ballistic missiles. Since Colonel Petrov had to go on a gut instinct to not fire back on the United States, we can assume that there was no proper disaster recovery plan to enact.

Roughly 89% of companies with an IT disaster recovery program test their program only once per year or never at all[8]. With a percentage like that, it is no wonder how events like the following IT disaster can occur. At Los Angeles International Airport, a network card malfunctioned, causing the U.S. Customs Service to lose access to its national servers and databases, as well as access to the local area network[9]. Due to Custom's inability to communicate, some 17,000 flights were either delayed or canceled, preventing passengers from getting to and from their destinations. Since there was no contingency plan in place, it took technicians 10 hours to find the culprit. Had there been proper contingency planning, U.S. Customs could have had a back-up system ready, a redundant connection to local area connections, and even different ways to connect to the national server.

Another example of an IT disaster occurred in a company where one of the authors of this study worked. The company (which will remain nameless!) implemented an IT disaster plan at his suggestion—it was a small company and he was the first full-time IT professional. The disaster plan included what to do for viruses, network shut-down, corrupted data,

6 Klein, M. "Green Bay Packers toughen defense with SaaS disaster recovery and business continuity plans" *WTN News*. Retrieved October 29, 2009, from http://wistechnology.com/articles/6670/

7 Barker, C. (2007, November 27). "The top 10 IT disasters of all time" | Tech News on ZDNet. *ZDNet Technology News*. Retrieved November 3, 2009, from http://news.zdnet.com/2100-9595_22-177729.html

8 Chisholm, P. "Ten Tips for Successful IT Disaster Recovery Planning." *Information Systems Security Today*. Retrieved November 4, 2009, from http://www.infosectoday.com/Articles/DRPlanning.htm

9 Abdollah, T. (2007, August 15). "LAX outage is blamed on 1 computer - The partial failure of a U.S. Customs network card led to the system collapse. City officials demand a full report and contingency plans." *Los Angeles Times*, pp. A4.

lightning storms, tornadoes, and fires. Every person was given their own user name and password with very specific, controlled access to databases and files allowing for easy tracking of who is doing what. However—he didn't plan for employee revenge in his IT disaster plan. An employee of the company was released for not being productive enough, which not surprisingly upset the now ex-employee. This former employee had just enough computer knowledge to open up a VPN from the company server to home, which they had previously done to be able to work from home. Our very new IT pro had failed to close off this VPN, allowing the former employee to still have potential access to the server, and had also failed to remove access to databases and files for that particular user. Within three days of the employee's termination, he began to notice files changing, databases losing integrity, and other questionable event on network bandwidth. At this point he was unfamiliar with employee malicious intent, but quickly understood the concept. After checking log files he found that this ex-employee was unable to cover their tracks and quickly took the necessary actions in order to prevent the former employee from gaining access to the files again. Lucky, he'd implemented a back-up program that he had not told anyone except the owner about. Although they lost three days worth of work, they were able to successfully recover all data that was tampered with. *[Editor's note: this was before he took my security management class: he knows much better now!]*

Honestly, it should be simple to understand the need for contingency planning. There are a multitude of problems in the world that can impact a company and their ability to access their information. Events ranging from a malicious packet to an acid rain storm, although may be seen as absurd, must be considered and allotted for in a firm plan for recovery. As can be seen in the three previous examples of IT incidents and disasters, some events can be successfully handled by having a decent recovery plan, and some events would still slip through the cracks. What is important to take away is that although no plan will cover every single possibility, a good plan will allow for most possibilities to be successfully navigated with little to no loss of information or productive time.

Proper contingency planning is a crucial element to every business today. In the 21st century, functional IT systems are essential to the everyday operation of almost everything. In the event of a disaster, outages and down time will significantly impact the effectiveness of any business. By creating a contingency plan and regularly testing it, companies can prepare themselves for disaster. Individual teams with specific assignments should regularly practice their roles to ensure readiness. Also, by utilizing online or off-site backup systems and SaaS packages, businesses can maintain operational functionality even through the disaster recovery process.

Always remember: *proper prior planning precludes poor performance.*

ABOUT THE AUTHORS

Joseph Carbon and Julian Hays are undergraduates in the Information Technology and Management degree program at Illinois Institute of Technology.

Ray Trygstad is the Director of Information Technology for Illinois Institute of Technology's School of Applied Technology and the Associate Director of IIT's Degree Programs in Information Technology and Management. He teaches courses in open-source operating systems; operating system virtualization; multimedia; information systems security management; and incident response, disaster recover and business continuity. He also teaches in the Master of Public Administration program at IIT's Stuart School of Business.

References:

Abdollah, T. (2007, August 15). "LAX outage is blamed on 1 computer - The partial failure of a U.S. Customs network card led to the system collapse. City officials demand a full report and contingency plans." *Los Angeles Times*, pp. A4.

Barker, C. (2007, November 27). "The top 10 IT disasters of all time" | Tech News on ZDNet. *ZDNet Technology News*. Retrieved November 3, 2009, from http://news.zdnet.com/2100-9595_22-177729.html

Biddinger, N. "The Information Technology Role in Disaster Recovery and Business Continuity "| Operations > Business Continuity from *AllBusiness.com*. Retrieved October 29, 2009, from http://www.allbusiness.com/company-activities-management/operations/6602879-1.html

Bradbury, C. "The IT disaster recovery plan." Retrieved October 29, 2009, from http://www.continuitycentral.com/feature0524.htm

Chisholm, P. "Ten Tips for Successful IT Disaster Recovery Planning." Retrieved October 25, 2009, from www.infosectoday.com/Articles/DRPlanning.htm

Hiatt, C. J. (1999). A Primer for Disaster Recovery Planning in an IT Environment. Hearsey: Igi Global.

Klein, M. "Green Bay Packers toughen defense with SaaS disaster recovery and business continuity plans." *WTN News*. Retrieved October 29, 2009, from http://wistechnology.com/articles/6670/

"Natural Disaster Preparedness Survey Spurs Scary Results For Atlanta." Retrieved October 29, 2009, from http://securitysolutions.com/news/natural-disaster-preparedness/

Trygstad, R. (2009, October 8). *ITM 478-578 Lecture 07*. ITM-478/578, Daniel F. and Ada L. Rice Campus, Illinois Institute of Technology, Wheaton, IL.

ABOUT ILLINOIS INSTITUTE OF TECHNOLOGY'S SCHOOL OF APPLIED TECHNOLOGY

Illinois Institute of Technology's School of Applied Technology offers hands-on, project-based technology-oriented education and training for both full-time students and working professionals. Courses are taught by IIT professors and industry professionals with significant working, teaching and research experience in their fields. The School of Applied Technology offers degree, non-degree, certificate, credit, non-credit programs, corporate training, short courses and seminars ranging from a few hours to several days in length. Both Bachelors and Masters Degrees are offered in Information Technology & Management and Industrial Technology & Management, as well as Undergraduate Certificates in Industrial Technology & Management, Graduate Certificates in Information Technology & Management topics and adult education/CEU courses in all fields. Our Information Technology & Management curriculum is supported by extensive dedicated laboratory facilities. We offer an comprehensive range of courses in information security and business continuity.

For more information on our education and training programs in information technology, please see http://www.iit.edu/cpd/

Illinois Institute of Technology (IIT) is a private, Ph.D. granting university founded in Chicago in 1890, offering programs in engineering, science, technology, architecture, design, psychology, public administration, technical communication, business and law.