Founded in 1970
pci GROUP
CELEBRATING 40 YEARS

August 17, 2011

Disaster Recovery/Contingency Planning: A Top Priority at PCI Group

By Robert E. Hufham, MA - Security and Compliance Officer

Recently, I had the opportunity to attend what turned out to be an extremely informative seminar on disaster recovery planning. The program, hosted by Pitney Bowes Mail Services, was held at the Hyatt Regency in Dallas and covered all of the most pertinent components of a sound disaster recovery plan. They include: infrastructure preservation, financial strategy, internal and external communications management, effective decision-making, balancing customer and organizational needs, and the regrouping/rebuilding phase following an incident. For attendees like me, the take away value was excellent.
While no one wants to experience a business interruption of any magnitude, they do serve as a learning lesson if well-documented and then analyzed carefully to assess the integrity of the disaster recovery/business continuity plan.

At the Pitney Bowes Mail Services' disaster recovery seminar, I learned that the company had such a lesson following the February 2011 fire in their Texas facility. The fire burned the facility to the ground, but did prove that Pitney Bowes' business continuity plan was sound. In a news release issued by the company regarding a new white paper it is offering on Best practices in business continuity, it noted "By following its own business continuity plan, Pitney Bowes minimized disruptions to employees, customers and the community. The work done at the destroyed building was rerouted to other locations, and a replacement site was on-line and operational within four months."

At PCI Group, disaster recovery and contingency planning has always been a top priority. We have implemented several measures across all the aforementioned pillars of disaster recovery preparedness and instituted policies and procedures to ensure our business continuity. A central focus point of all of our planning is protecting our customers' data. It is our most important commodity. In place at PCI is a very robust, well-managed remote back-up site where all of our customers' data is backed up to tape. In the event of an incident, we know our customers' data is protected.

At PCI Group, we have established disaster recovery/business continuity protocols. They encompass the set-up of an Emergency Operations Center (EOC) situated in a 6,000 square foot common room and specified adherence to specific tasks and procedures. The emergency diesel generator feeds our Uninterruptible Power Supply (UPS) which, in turn, feeds power to our server room, the adjacently-located EOC, and other essential areas. Both the server room and EOC have independent, self-contained HVAC systems to maintain proper operating temperatures. As an added precaution, all of our facility's security systems (i.e., card key access system, time and attendance terminals, biometric identity scanners, security camera system, etc.) are on back-up whereby we do not lose any of our security functionality. Our protocols also specify that our resources be directed to the EOC based on a priority schedule consistent with our primary mission of protecting our customers' data and keeping our customers' informed at all times.

Sound disaster recovery/business continuity planning is also a function of comprehensive risk assessment. Based on having performed a thorough assessment of potential threats, we are able to effectively triage and respond to most anticipated incidents. As a result of our continuous risk assessment, we make additional improvements to our facility to mitigate any potential vulnerability.

For example, we deemed a number of exterior doors, which provide for emergency egress, to be somewhat compromised in terms of their water-tightness due to weathering and age-related wear. As a result, we replaced those doors with new doors that are more storm and water-resistant and feature high performance sealing and threshold plates. As part of our disaster recovery/business continuity plan, we evaluate the various physical and procedural components of our plan on an annual basis to ensure their full integrity. Additionally, we regard each incident as an opportunity for a learning lesson and other possible enhancements to the plan.

When an incident occurs, PCI first relocates its customer service – the hub of our daily operations – to the EOC so that it is fully-functional in terms of Information Technologies (IT) and telecommunications systems. Next, we focus on our developers and programmers and their continued operations during the incident period. As an additional measure, we are currently re-engineering our electrical supply on the back-up system so that our cargo elevators can be utilized to move mail through our facility in the most efficient way during a potential disaster.

During late spring this year, the southeastern United States experienced severe thunderstorms causing multiple regional power outages. At PCI Group, we incurred one such outage lasting16 hours. By implementing our recovery plan, we were able to maintain operations; however, we also took advantage of what we learned and incorporated these lessons into our plan.

For example, PCI has in place an emergency diesel generator with a seven-day fuel capacity. Without knowing just how long we would need to operate the generator and considering that in a regional power outage demand for refueling would be very high, we insured that we scheduled a fuel delivery in ample time. Also, during this power outage, we realized that there were certain areas of our building which would need additional back-up lighting. We used the opportunity to identify those areas where the lighting should be augmented, and then photo-documented them down to the socket. Consequently, we established an accessible, central storage area to house all of the lighting peripherals (e.g., power cords, lamps, flashlights, etc.).

We also capitalized on this incident to refine our internal communications procedures. We established a communications plan for the EOC that instituted a central coordinator to collect reports from onsite managers and relays information to the onsite leader. The coordinator also passes information and directives back to onsite managers. The onsite leader is responsible for decision making, communicating with offsite executives, and external communications. By implementing this plan, we have created clear and efficient communication flow to internal and external stakeholders.

Because PCI Group has followed the proper due diligence in establishing a sound disaster recovery/business continuity plan, we are extremely transparent in our communications with customers regarding incidents. They are kept informed about what has happened and how we are operating on their behalf. We are always honest about what we can and cannot do in the face of an incident, and fully cognizant of our customers' need to maintain their business continuity even as we address the incident.

All businesses, regardless of their size or industry, should have a well-developed disaster recovery/business continuity plan in place. The plan should be tested and practice drills conducted to make sure all staff mem-

-bers understand the proper procedures to follow. These practice drills and subsequent reviews of the plan also provide an opportunity to adjust those areas where weaknesses may have been revealed.