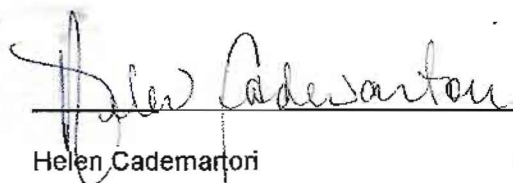


IT Division Safety Self Assessment

FY10

Measure 3: Emergency Preparedness of IT Data Centers

Reviewed and Approved:

 9/24/10

Helen Cademartori

Date

IT Business Manager

 9/24/10

Ann Tomaselli

Date

IT Safety Coordinator

Emergency Preparedness of IT Data Centers

August 27, 2010

Executive Summary:

IT manages four data centers, all in the 50 complex. These data centers house numerous critical business, financial and scientific systems and comprise tens of millions of dollars of equipment. In the event of a fire, earthquake, or other emergency, are the procedures and systems in place for shutting down, and/or bringing back up these data center in place? And are they clearly documented, and understood by the occupants? While the individuals in charge of these systems are knowledgeable and able to balance priorities, there are still some gaps that need to be addressed. IT has the necessary systems in place to protect equipment and personnel, but the procedures to be undertaken in the event of an emergency are not formally documented. IT needs to review who currently has access to each of the data centers, and to document and communicate a policy and a process for enforcing/maintaining data center access. The Facilities Division, as the owners of the halon systems in 1156 and 1275 should review if it needs to be tested, and if so schedule the test.

Introduction:

In February at the Joint Genome Institute (JGI), about 200 computer servers sustained water damage when a fire sprinkler head located above the servers activated and discharged approximately 1,000 gallons of water. Firefighters from the Contra Costa County Fire Department arrived at the scene and entered the building. They determined there was no fire and shut off the sprinkler control valve. The building manager activated the Emergency Power Off switch and shut down all the computer equipment in Room 422 and the adjacent larger server Room 421, which was not affected by the sprinkler water. All flooded areas were cleaned up. The sprinkler head activation was triggered by an overheated server room, because two chilling water valves appeared to have been improperly closed, which would have left the room with no cooling capability. There were no injuries and property damage involved mostly the servers.

Focus Area:

The Division owns or operates several data centers that provide service to line operations. Broad-scale (i.e., earthquake, fire, weather, etc.) as well as local-scale (electrical failure, plumbing failure, etc.) have the potential to shut down operations for extended periods of time. Given the Division's mission, the ability to respond to emergencies safely and efficiently represents a potential liability.

This self-assessment will focus on emergency readiness and will address two elements: (1) adequacy of procedures/systems designed for operational response to emergencies within the division and (2) adequacy of procedures designed to protect the safety of Division employees during and immediately after an emergency.

Current Requirements:

At LBNL we follow the National Fire Protection Standards as mandated by DOE. In particular NFPA 75, *Protection of Information Technology Equipment*. IT however does not have formal written procedures related to access of the data centers. It does require those who are given access to review how to disable the halon for the room if necessary.

Assessment Scope:

The IT Division has four separate data centers. The primary one which we are responsible for is 50B-1275. IT also operates a communication node in 50-1156. There is a small co-located space in 50A-2109C, but the equipment here is primarily non-IT. There is a data center in 50B-2265 where IT has equipment, but the space is run by Computing Sciences. The scope of the emergency preparedness assessment is limited to 50B-1275. This is the facility that would have the most significant impact on the institution, should there be an actual emergency.

Assessment Results:

Procedures are in place for data centers operated by IT. They are not formally documented and need to be so that any who have access to the spaces will understand the hazards that they could be exposed to or responsible for.

The data centers at the Laboratory main site are all monitored by the facilities department on a 24 hour basis. In the main data center (1275) the individual computer room air conditioners (CRAC) are monitored, as well as, the supply and return water temperatures and all pumps and fans used for the heat exchanger and cooling towers. The 1275 room is also monitored for fire and smoke with several levels of detection. There are also standard and high sensitivity smoke detectors throughout the room, as well as high heat detectors. Suppression is handled by emergency power off for the entire room, halon and sprinkler system as a last resort. In 1275 IT also has room and equipment temperature monitoring throughout the room. The IT sensors are mainly used to monitor temperature in the hot and cold isles and equipment sensors mainly to ensure proper air temperature is flowing across the CPU's. Both can be used to identify high heat condition in the room and used to notify facilities. The facilities monitoring is handled via special hard wired circuits and paging, while IT monitoring is handled via the network using email and paging.

The various alerting systems currently are not connected as they need to be "tuned" to the room to avoid erroneous pages/emails that can lead to paging fatigue by responsible parties. This is being reviewed between IT and Facilities so both sides have the information they need.

Approval of access to 1275 is handled by two individuals. The Building Manager for the 50 complex and the Data Center Manager from IT. There is no physical key access to 1275 only card key access. This access is granted by the two mentioned individuals. The interest is in limiting access to those who will be working in the room and if they are working in the room, ensure via training, that they know the hazards and how to address them should they arise. There is training that is required to anyone working extensively on equipment in the room. This training is EHS 361. There are individuals however, who have not taken this training and have access. This appears to be a legacy issue which needs to be addressed as well as a programming issue. For example, executives are given blanket access to certain areas which include the computer data center. Blanket access should be reviewed as to how to limit the access to 1275. Also a way to manage what facilities individuals may need access and if they should be required to have any particular training should be addressed.

The halon fire suppression in 1275 is owned by Facilities. Currently testing on the system has shown alarms and sensors can be triggered. There is the halon agent available. The question currently outstanding is whether the triggering of the halon would actual result in deployment. There are ways to test this but due to the nature of the gas as well as the expense of the test, the test has not taken place.

Findings:

Card key access is approved by two individuals. The list of those who have access has not been scrubbed recently, and the not all of those who have (and need access) have completed all required trainings. This needs to be corrected.

Policy for computer room access is unclear and unwritten. Policy needs to be formalized and communicated.

The halon system in 1275 is expensive to test. Certain potential single points of failure have been identified. This could leave life and equipment in danger of being destroyed in the event of a fire should one occur and the system fails.

Observations:

There is currently no way to discriminate between a low level and a high level alert, and there is the potential for recipients to experience "alert fatigue" and overlook a critical alert. The system needs to be tuned.

24 x 7 support is currently one person with after hours "best effort". Unclear if this is "acceptable". This may be addressed in formalizing processes and procedures noted in "findings".

Facilities and IT aren't fully integrated with monitoring of data center. This is being reviewed as to how best to rectify.

Recommended Corrective Actions:

Formalize and document processes and procedures required for access to 1275. Formalize if this needs to be across divisions. (CATS item 8218)

Test halon and heat sensors in 1275 to ensure systems are working as expected. (CATS item 8220).

Card key access is approved by two individuals. The list of those who have access has not been scrubbed recently, and the not all of those who have (and need access) have completed all required trainings. This needs to be corrected. (CATS item 8226)

Noteworthy Practice:

The day to day maintenance of the space can be a challenge e.g. when new equipment is received a great deal of packaging can build up. This has partially been remedied by receiving most equipment in a secondary location and staging it when it needs to be installed.

Conclusion:

IT has the necessary systems in place to protect equipment and personnel, but processes of these systems have not been formalized or documented. IT needs to review the access to data centers, set and document a policy and communicate to all parties. Facilities as owners of the halon system should review if it needs to be tested, and if so schedule the test.

Lines of Inquiry

In an effort to keep the focus on "Emergency Preparedness" we looked at the following two questions:

1. What sort of systems are in place to protect equipment and personnel?
2. How do we know those systems work?

Self-Assessment Methodology:

1. Person(s) conducting self-assessment: Division Safety Coordinator

2. Techniques to be used during the self-assessment. Possible techniques include but are not limited to:

- Documentation Review
 - i. NFPA 75 Standard for the Protection of Information Technology Equipment 2003 Edition (pending 2009)
 - ii. Data Center Monitoring Matrix
 - iii. JHA EHS 361 compliance
 - iv. 1275 access log from Building Manager
- Personnel interviews/questionnaire
 - i. Data Center work leads
 - ii. Interviews of SME and super-users