Claremont McKenna College
Information Technology Services
Disaster Situation Response and Data Protection Plan
Five Levels of Disaster Classification and CMC ITS Disaster Recovery Response

Rev. July 2, 2009

In this document, we describe five classification levels of disaster recovery response modeled on disaster situation response plans originating in the military, which we have fine-tuned to meet CMC Information Technology circumstances.[1]

ITS Responses to Disaster Situations

Level One Disaster Classification: Threat of disaster without evidence

The Level One Disaster Classification encompasses those incidents in which no damage to any data systems occurs, nor is there any proof of attack, yet circumstances are such that there may be a publicity or regulatory concern. One example could be posted boasts about incursions into the CMC network on blogs or Web forums, or claims that proprietary data were compromised, yet without evidence. An example of a Level One Disaster Classification that took place at CMC occurred in November 2006. There was a rise in spam, leading to some concerns that CMC servers may have been hacked. One major issue with such “suspected but no evidence” disasters is that it can be difficult to prove or disprove them.

In Level One cases, the procedure for ITS is the following:

1) If necessary, ITS Senior Staff (CTO, Directors of ISNS and ITCS, and the Business Manager) will meet or share information to craft a response.
2) The problem is identified, and an assessment of the situation is determined as accurately as possible.
3) The appropriate parties requiring a response are identified.
4) An accurate and direct response is composed and sent alerting the appropriate parties of a) the perceived problem; b) our findings; and c) what they can expect in terms of current and future service.

Scheduled outages due to maintenance or upgrades may lead to persons assuming a disaster if they are not made aware of them. Therefore, it is ITS policy to follow the steps above in advance of the scheduled outage, and send end users that may be affected an e-mail describing the date and time of the expected outage, who and what services will be affected, and the purpose of the scheduled outage. After restoration of services, a message with details about the outage will explain what actually occurred (e.g., all went normally according to expectation or there were substantial deviations from what was anticipated) to the constituencies affected.

[1] Much of the discussion below is summarized from Mike Talon’s work located at http://techrepublic.com.com/5171-22-1033007.html. Talon based his suggestions loosely on a British military classification system for threat levels in battle situations.

Level Two Disaster Classification: Actual attack without data loss

CMC's ITS Department has taken many security measures and uses penetration-testing tools to ward off those disasters classified as Level Two: when an attacker actually has breached an institution's security digitally and there is evidence of the attack. In these cases, there is clear proof of the attack, but the extent of the attack must be investigated, and any infected files or server systems quarantined.

Viruses/Trojans: Since many end users (students, staff, and faculty) have varying levels of protection on their systems, it is a routine occurrence to find some infected systems with viruses attempting to hook up to our network, thus imperiling other systems. For virus attacks, ITS imposes immediate quarantine as necessary both for infected files and for infected server systems to inhibit the spread of the infection across the College. This may mean quarantining completely some end users, including the suspension of their e-mail service, locking them out of file servers, and taking other actions that interrupt production for our users until the virus problem is addressed. The persons affected in the quarantine are notified, and staff members are dispatched to assist. For example, students may be given explicit directions on how to remove viruses from their infected system, or they may be assisted by Resident Technology Assistants, or at times, an ITS staff member. Information may be shared among ITS members about patterns in viruses found on campus. If deemed appropriate -- for example, there is a clear pattern of very bad viruses that can and should be prevented -- an e-mail warning end users is produced detailing information about the virus and steps to prevent it, and staff may be dispatched to ensure end users are appropriately protected. Normally, such decisions on whether to send an e-mail to end users and what to communicate are made by the Assistant Director of ISNS.

Network intrusions: For network intrusions, in addition to quarantining the affected systems, Network Services seeks to identify the security hole that the intruder used, and steps are taken to patch the problem to ensure other potential hackers cannot come in the same way. After the original attack, ITS staff members next investigate and identify the full extent of the intruder's penetration, and taking preventive measures to make sure the same kind of attack cannot occur again. All steps will be completely documented digitally for future reference. Since network intrusions are specific attacks on our institution, ITS will as standard procedure attempt to find out the identity of the intruder.

In addition to the measures identified above for Network Services staff, Level Two Network Intrusion cases require the following additional steps:

1) If necessary, ITS Senior Staff (CTO, Directors of ISNS and ITCS, and Business Manager) will meet or share information with fellow staff as necessary to craft a response.
2) The problem is identified, and an assessment of the situation is determined as accurately as possible, including how far the hacker got into the network, what they

saw, and what, if anything, they took. Appropriate ITS staff will be asked to show what happened and how.

3) Parties directly affected are notified, and a plan of remediation is discussed, agreed on, and followed.
4) The appropriate parties requiring varying degrees of notification and disclosure are identified.
5) Accurate and direct responses are composed and sent alerting the appropriate parties according to the degree of disclosure necessary of a) the perceived problem; b) our findings; c) what steps we took to remediate the problems; and d) what they can expect in terms of current and future service.

Level Three Disaster Classification: Minor data/system loss

Level Three Disasters occur when data systems and data are lost to natural causes, attacks, or system failures, but are contained to mostly smaller-scale issues. By definition, "smaller-scale issues" are defined as the loss of non-critical systems or a single critical system that can be restored quickly. The key difference between Level Three Disasters and those that follow is its classification of response: high priority, but not high urgency. The Level Three classification assumes that end users can continue to do the majority of their jobs without this data and/or without these systems, but that staff must still get them back up and running or find out what was lost. If a minor data or system loss occurs but its Recovery Time Objective is at least one business day, and it does not require additional infusions of capital, its recovery can be scheduled and ITS has time to react and correct the problem, thus not meriting a Level Four designation.

The procedure for ITS in these cases is to first determine the problem, its extent, what measures may be required to ensure restoration, and ensure the damage is contained. For example, this may require verification of backup systems for other data systems, test restorations of controlled and previously backed-up data, and determination of what caused the system failures. If e-mail is not compromised, an e-mail alerting affected staff, faculty, and/or students to the problem is crafted and sent, normally by the Director of ISNS or his designate directly without need for meeting with fellow ITS staff. If addressing the problem will require rebuilding the affected systems or affect other services to bring our systems back, the e-mail will describe potential downtimes and seek to minimize inconvenience to end users. Updates will be sent as necessary to inform constituents of the extent of outages.

Level Four Disaster Classification: Major data/system loss

Level Four Disasters are larger-scale disasters involving multiple critical systems that fail at the same time, due, for example, to power loss, fire, or flood in the data center. Level Four Disasters are those in which ITS can correct for the issues, and it does not require additional infusions of capital, but an immediate response is required to get business-critical systems back up and running. Systems that have a Recovery Time Objective of less than one business day fall into this category when they fail (for example, full loss of e-mail for large segments of end users, or the web going down).

The procedure for ITS in Level Four Disasters, as with earlier versions, is to determine the problem(s), extent, what measures may be required to ensure restoration and contain damage, but with an “all hands on deck” response, acting quickly to restore as much of the data and services as quickly as possible so that end users can resume working with those systems.

If e-mail is not compromised, an e-mail alerting affected staff, faculty, and/or students to the problem and expected resolution is crafted and sent, normally by the Director of ISNS or his designate directly without need for meeting with fellow ITS staff. If there is no email availability, our hosted emergency notification system (Connect-Ed) or some other means of communication may be used. If addressing the problem will require rebuilding the affected systems or affect other services to bring systems back, an e-mail or some other means of communication will describe potential downtimes and seek to minimize inconvenience to end users. Updates will be sent as necessary to inform constituents of the extent of outages as well as returns of service. In Level Four disasters, a thorough investigation is completed after the restoration of critical services, and documentation made and preventative steps taken both to avoid repeated occurrences and to improve responses in similar situations in the future.

Level Five Disaster Classification: Total loss

The highest level in the system, a Level Five classification is invoked only in cases where a disaster causes massive disruption in services. Causes might include earthquakes, large-scale floods, and fires. Level Five disasters usually involve loss of both data systems and physical plant, including buildings. Due to considerations such as loss of work space, loss of life, and psychological impact, recovery is difficult.

True fail over to another data center is sufficiently costly that we will have to plan for it in stages. At the current time, in the event of a Level Five disaster, CMC would seek to come back via a recovery effort rather than a complete failover exercise.

ITS keeps weekly backup tapes and other copies of CMC data off-site. In most Level Five Disasters, we expect that at most only one week’s of data would be lost, and that ITS employees would eventually be able to recover our data to new systems from these copies warehoused off-site after they're returned to us by the contractor. However, since our off-site facility is still regional, should that service be compromised, we could end up in a position that would imperil restoration.

If ITS employees are no longer available to enact a Disaster Recovery Plan, successors will need to act as quickly as possible, given the situation, to find new staffers or temporary employees, train them, and restore services.

Communications will be sustained by hosted emergency notification system (Connect-Ed).