Incident Management Procedures

v8.0

Information Security Office
The University of Texas at Austin

Last updated: February 2012
Originally Created: September 2005

I. Introduction and Overview:

Incident management is needed to assure continued operations in the event of a security breach or incident involving a computer virus, worm, or other attack against university information systems, or misuse of information technology resources. As specified by the UT Austin Information Resources Use and Security Policy, UT System UTS-165, and Texas Administrative Code 202 (TAC202), the Information Security Office is required to establish and follow Incident Management Procedures to ensure that each incident is reported, documented, and resolved in a manner that restores operation quickly and if required, maintains evidence for further disciplinary, legal, or law enforcement actions.

II. Purpose:

The purpose of this plan is to facilitate The UT Austin's rapid response to and management of computer security incidents by:

- Monitoring the University's information technology (IT) resources to detect computer security threats.
- Assessing severity level, type, and scope of threats.
- Alerting constituents of threats, in a manner consistent with severity level, type, and scope of threat.
- Providing up-to-date information that allows rapid response and increases ability to avoid, alleviate, or contain the threat.
- Determining whether law enforcement is likely to become involved, and if so, preserving evidence.
- Keeping complete records of actions taken to address the threat.
- Containing or eradicating the problem.
- Restoring function.
- Preventing recurrence.
- Preserving evidence, if law enforcement is likely to become involved.
- Conducting post-mortems and applying the lessons learned from them.
- Minimizing loss of time, money and data as a direct or indirect consequence of the threat.
- Fostering an organized and professional response to the incident based severity level, type, and scope of the threat.

III. Scope:

This plan applies to owners and custodians of IT resources at the University of Texas at Austin, the Information Security Office, students, faculty, staff, and others who use the university's IT. A computer security threat is defined as an event causing actual or potential harm or new and noteworthy information that may negatively impact IT resources. Examples include, but are not limited to, instances of disruption or denial of service; attempts to gain unauthorized access, or unauthorized changes to hardware, software, or data.

IV. Authority:

The sources of authority for the Incident Management Procedures are laws of the State of Texas (TAC202), UT System UTS-165, and UT Austin's Information Resources Use and Security Policy. Responsibility for implementation rests with the UT Austin Chief Information Security Officer.

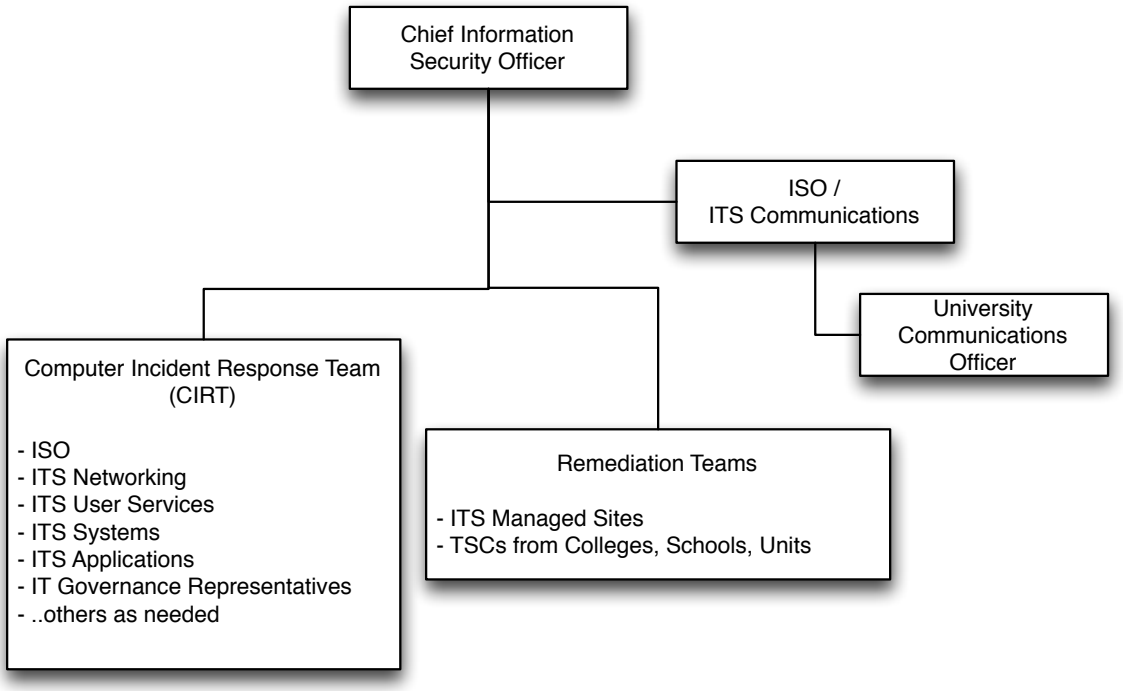
V. Escalation Path and Information Flow

In the case of a computer security incident, contact the Information Security Office (security@utexas.edu | 512-475-9242).

For sever or very severe incidents, it is prudent to contact the Chief Information Security Officer directly at:

Cam Beasley
Chief Information Security Officer
UT Austin
512-475-9476
cam@utexas.edu

The following highlights a general flow for incident related information. Some communication components could be removed in the event of a lower threat incident.



VI. Computer Incident Response Team (CIRT) Members

The typical threat assessment levels of most computer security incidents fall in the range of "very low" to "moderate". In such events, the basic steps of identification, notification, communication, containment, eradication, and recovery are usually not overly complex. In such cases, the Information Security Office if tasked with reporting the incident, reducing impact of the security incident (e.g., setting network quarantine), and ensuring the respective unit is able to remediate the problem.

Occasionally, however, a security incident progresses to a severe or very severe level. In such cases, speed, preparation, organization, and a clearly articulated plan are required. The Incident Management Procedures are mainly concerned with responding to computer security incidents in severe and very severe situations. When such events occur, these procedures are activated; the Computer Incident Response Coordinator assembles the Computer Incident Response Team (virtually or in person), and appoints the Communications Coordinator and a Lead Incident Handler from the Information Security Office. Other groups or individuals external to ITS may be called in as needed.

Information Security Office

Computer Incident Response Coordinator (CIRC) – The Chief Information Security Officer (CISO) or a person designated by the ISO shall serve as Computer Incident Response Coordinator, who makes decisions and coordinates the University's response to a severe or very severe computer security incident. The CIRC consults with and provides continuing updates to the university executive leadership. If the CISO is unavailable and a substitute has not been designated, another member of the Information Security Office will serve in this capacity. The CIRC is responsible for assembling the Computer Incident Response Team, assigning tasks, and making critical decisions. The members of the Computer Incident Response Team will vary depending on the type and severity of the incident. The CIRC shall appoint the Communications Coordinator and a Lead Incident Handler. If necessary, the CIRC will help assemble departmental Remediation Teams and coordinate their efforts.

Communications Coordinator (CC) – The CIRC shall appoint a Communications Coordinator to lead and direct the incident communications. Depending on the nature and scope of the incident, the Chief Communications Officer may be contacted by the CC. The CC coordinates the communication of timely and accurate information during an emergency and directs media inquiries to the appropriate person(s). Depending on the nature of the emergency, electronic mail, Web pages, possibly, phones and faxes may be unavailable as a means of communication. The CC should be prepared to utilize many different avenues of communication to spread the word. Consistent with the provisions of this section, the CC shall have the authority to assemble a communications team, delegate tasks, and take other actions as required.

Lead Incident Handler (LIH) – Generally, the CIRC shall designate a member of the Information Security Office to lead the Computer Incident Response Team and provide technical expertise in identifying, diagnosing and creating a detailed technical plan of response to the incident. The LIH should have the technical skills to distinguish a real attack from a hoax, quickly assess the scope of the incident, and identify critical systems or services that may be at risk, and provide content for dissemination by the CC and leadership in training on-site Remediation Teams.

Computer Incident Response Team (CIRT) – For low to moderate threat situations, the Computer Incident Response Team may only consist Information Security Office staff. Otherwise, membership will vary depending on the nature and type of the incident.

Department Based

Remediation Team(s) – On-site teams isolate, eradicate and facilitate recovery from a computer security incident. Remediation Teams should have both the technical skills to carefully and methodically deal with attacked systems and the customer service skills to reassure users during a potentially stressful period. The members of these teams should have a calm and professional demeanor and the ability to work quickly but accurately.

University Communications

The Chief Communications Officers will be informed of severe or very severe incidents and will assume responsibility for media contact.

VII. Threat Assessment

i. Associating threat levels to incident response

A reasoned approach to computer security incidents gauges the level of response to the danger posed by the emergency. An incident that is not widespread and does not cause significant damage should not receive the same degree of response or the same commitment of human and computing resources as a very dangerous exploit or mass-mailing worm affecting many computers at UT Austin. Likewise, a vulnerability that gives the attacker complete control over computers should receive a high level of attention. The Computer Incident Response Team will assess the risk posed by each malicious program or computer emergency as soon as it is detected. The threat assessment will be updated as the situation warrants.

Threat assessment is an inexact science. For each incident, the number of computers potentially affected, the number actually affected, and the potential damages are all unknown to a certain extent. The Computer Incident Response Team, operating with imperfect knowledge, must make reasonable estimates of each of the factors and use those factors to formulate a necessarily inexact threat assessment. As more information becomes available and as the nature of the threat evolves, the assessment team will modify the threat assessment. While threats usually diminish as the incident in contained and eradicated, some exploits and destructive devices develop variations or new features, making them more of a threat.

The Computer Incident Response Team will consider a number of factors in determining the threat posed by a computer security incident. The threat components are grouped into two categories: the probability that damage will occur, and the severity of the damage if it does occur.

ii. Factors affecting the probability that damage will occur:

- Prevalence and distribution of the destructive devices. Exploits for which scripts have been widely and publicly distributed are a greater threat than those that have not been scripted or for which the scripts are closely held.
- Risk of sensitive university data loss will be considered.
- Rate of propagation. Flash or connectionless worms have the potential to infect tens of thousands of computers within a few minutes. Distributed denial of service (DDoS) zombies can be widely activated to generate crushing network attacks almost instantly.
- Distribution of affected platforms at UT Austin. Common operating systems, such as Microsoft Windows and applications, such as Internet Explorer, could affect more users. Hardware, operating system, network protocol and application(s) used in the propagation of the malicious software or vulnerability are altogether considered the computing platform.
- Number of people potentially affected by incident. A destructive device that incapacitates a network device on the campus backbone network would be devastating, while a virus infecting a single user workstation would generally impact only that user.

- Multiple propagation avenues. An example would be a destructive device that spreads both as an Internet mass mailer and network drive infector.
- Complexity or resistance to detection. Some destructive devices are multipartite, some use cloaking, stealth, or randomization to conceal and disguise themselves.

iii. Some types of serious damage that may result from a security incident:

File or File system damage – Non-repairable file destruction or modification (e.g., zeroed file length, overwritten file content) is worse than repairable file modification (e.g., changed file name).
Network or server congestion – Some incidents produce a high volume of network or server traffic, reducing availability of the computing resource and interfering with the university's mission.
Non-repairable hardware damage – Complete destruction of hardware and data, such as erased or scrambled Flash-BIOS.
Disclosure or compromise of data – Compromised personal, confidential or sensitive information, such as username/password combinations, bank account and credit card information, or information designated confidential or sensitive by state or federal law.
Difficulty of eradication – Some malicious software such as boot record infectors and memory resident viruses are very difficult to remove, requiring procedures not recommended for the casual.

iv. Classification of probability:

Low: Insignificant number of infected computers, non-virulent (e.g. Trojan horse), easy detection, uncommon computing platform.
Medium: Significant number of affected computers and geographical distribution, moderately virulent (e.g., virus), moderate difficulty of detection
High: Great number of affected computers and common platforms, wide geographical distribution, highly virulent propagation, difficult detection (e.g., NetBIOS vulnerability).

v. Classification of damage:

Low: No destructive payload or incidental damage, easy removal.
Medium: Non-destructive trigger, isolated file modification or repairable file damage, moderate difficulty of removal.
High: Destructive payload including extensive or non-repairable file destruction or modification, very high server or network traffic, non-repairable computer damage, large-scale security breach, difficult removal.

vi. Threat Assessment Level Determination

Severity of Damage	Probability of Occurrence: Low	Medium	High
Low	Very Low	Low	Moderate
Medium	Low	Moderate	**Severe**
High	Moderate	**Severe**	**Very Severe**

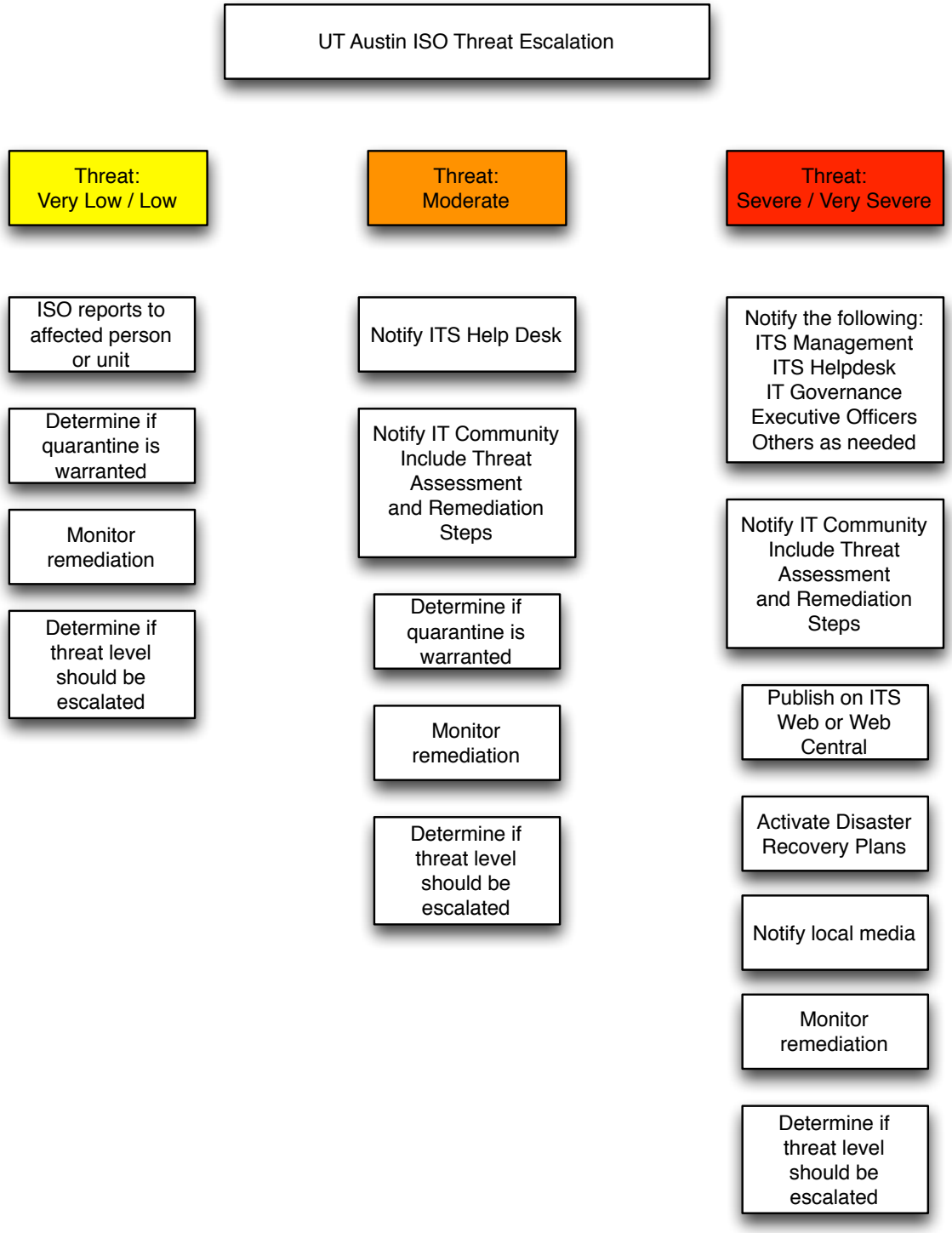
vii. Response Levels

Very Low: Characterized as not dangerous and not widespread. No response required except addressing the immediate problem by notifying those responsible for the equipment or resources involved, who then resolve the problem.
Low: Characterized as either moderately dangerous or moderately widespread, with low severity of damage or low probability of occurrence. Post alert on Security Alerts web page or send e-mail alert to the IT community within a day of detection. Apply network quarantines as necessary.
Moderate: Characterized as either dangerous or widespread or virulent. Post e-mail alert to IT community the same day as detection. Post alert on ITS web pages the same day as detection. Recommend update to appropriate virus definitions, security patch, Hotfix, service pack, etc. at weekly update, or otherwise, as soon as possible. Apply network quarantines as necessary.
Severe: Characterized as highly dangerous and either highly widespread or very virulent. Post Spotlight on Web Central within hours of detection. CIRC assembles team and plans response. Recommend immediate updates of virus definitions, security patch, Hotfix, service pack, etc. as appropriate. Ensure appropriate software updates are available. Apply network quarantines as necessary.
Very Severe: Characterized as highly dangerous, widespread, and virulent. Post Spotlight on Web Central within hours of detection. CIRC assembles team and plans response. Urge immediate updates of virus definitions, security patch, Hotfix, service pack, etc., disk or network security scans, and possible large-scale network isolation. Business continuity plans may be invoked.

viii. Examples of threat assessment levels: "very low" – "very severe"

Very Low: - W32/Fbound virus. While not only in sent in Japanese, this mass-mailing worm does not carry any damaging payload.
Low: A localized web site defacement. A localized macro virus tries to delete all files on the C: drive by using the DELTREE command. Runs only on Asian versions of Microsoft Word.
Moderate: Mass-mailer that attaches itself to outgoing e-mail and spreads widely. No destructive payload. A system infected by a drive-by download made possible by outdated browser plugins.
Severe: W32/Blaster worm This worm exploits a vulnerability in Microsoft's DCOM RPM interface and affected thousands of systems on the Internet. The publicized malicious code was able to quickly propagate resulting in many compromised systems.
Very Severe: A Zero-day exploit is found active in the wild that allows remote arbitrary code execution on all recent Microsoft Windows platforms that are exposed to the Internet. The vendor indicates they will require several days to release the necessary security software patch.

IX. ISO Threat Escalation Plan



X. Phases of Response Plan

1. Identification and Notification

1.1. Determine risk of continuing operations.

1.2. Assemble the Computer Incident Response Team.

1.3. Determine the nature and scope of the incident with an appropriate initial threat assessment level. Continue to monitor for changes in threat assessment, making modifications as required.

2. **Communication and Containment**

2.1. Determine Technical Plan of Action.

2.2. Determine available communication avenues, and whether alternative forms of communication are required.

2.3. Reserve a Training/Information Sharing Room.

2.4. Occasionally, severe and very severe incidents will be discovered that have not received wide publicity. Should the circumstances be such that widespread publicity of a vulnerability could have an adverse affect – even attracting attention likely to make UT a target of a severe attack – the CIRC and CIRT will notify the university executive leadership. Information will be distributed on a need-to-know basis for a reasonable period until the threat is contained. Executive Officers and IT Governance chairs will be informed of the event, given the reason for need of careful handling, and will receive updates as the situation progresses.

2.5. Except in exceptional circumstances delineated above, communicate with University community, based on current threat assessment and technical plan, to help prevent the spread of the attack.

2.6. Conduct training sessions and disseminate technical support information.

2.7. Take the necessary steps to keep the problem from getting worse (e.g., port filters, quarantines).

2.8 Determine if Data Breach Notification Plan should be activated (i.e., if protected personally identifiable data has been exposed).

3. **Eradication and Recovery**

3.1. Coordinate response.
3.2. Ensure system integrity; maintain user data.
3.3. Determine cause of incident.
3.4. Improve defenses.
3.5. Perform security assessment of systems/networks.
3.6. Remove cause and correct any changes it has made.
3.7. Restore operating system and applications as necessary.
3.8. Install service packs, Hotfixes, or security patches as necessary and recommended by vendor.
3.9. Restore user data from backups as necessary.
3.10. Bring systems back online.
3.11. Change all passwords.
3.12. Monitor system performance and report activities.

4. **Follow-up**

4.1. Conduct a post-mortem meeting.
4.2. Produce a follow-up report.

XI. Outline and Task Checklist

The following is a suggested outline of tasks to be completed by the Computer Incident Response Coordinator (CIRC), the Communications Coordinator (CC), the Lead Incident Handler (LIH), the Computer Incident Response Team (CIRT), and the Remediation Team(s). This list should be modified as the situation warrants.

1. Identification and Notification

1.1 Determine risk of continuing operations. [Decision point: Shut down the system? Disconnect from the network? Continue operating to monitor subsequent activity?] The CIRC is authorized to ensure that this is addressed as soon as possible.	
1.2 Assemble the Computer Incident Response Team (CIRT). The CIRC appoints a CC and LIH and coordinates the implementation of this plan. The CIRC may call upon on the CC to assist in contacting members of the team.	
1.2.1 Organize and Alert Remediation Teams. The CIRC will perform this task, but may call upon the CC to assist in contacting members of the team.	
1.2.2 Work with Chief Communication Officer to designate a Media Contact, as needed.	
1.3 Determine the nature and scope of the incident with an appropriate initial threat assessment level and monitor throughout containment stages, making modifications as required. The CIRT is responsible for this task. The CIRC should remain in contact with the CIRT to stay appraised of the situation.	

2. Communications and Containment

2.1 Determine Technical Plan of Action. The CIRT formulates a detailed technical plan of action or evaluates and recommends adoption of such a plan developed by an outside source and submits it to the CIRC for approval.	
2.2 Determine available communication avenues, and whether alternative forms of communication are required.	

2.3 Reserve the Training / Information Sharing Room. The CC will handle reserving a room for use by the CIRT.	
2.4 Occasionally, severe and very severe incidents will be discovered that have not received wide publicity. Should the circumstances be such that widespread publicity of a vulnerability could have an adverse affect – even attracting attention likely to make UT-Austin a target of a severe attack – the CIRC and CIRT will notify executive leadership. Information will be distributed on a need-to-know basis for a reasonable period until the threat is contained. Executive Officers and IT Governance Chairs will be informed of the event, given the reason for need of careful handling, and will receive updates as the situation progresses.	
2.5 Except as otherwise provided in Sec. 2.4, communicate with University community in accordance with the Notification Scheme's threat assessment model.	
2.5.1 Post notices on the web (WebCentral/ ITS/ External Emergency Site). The LIH should provide content for these web pages. The CC will handle getting it posted.	
2.5.2 Send notices to mailing lists. • Send notice to ITS Staff: its-staff@its.utexas.edu • Send notice to Executive Officers: VPCouncil@po.utexas.edu • Send notice to departmental technical contact mailing list at: it-talk@utlists.utexas.edu • If warranted, send notice to all students, staff, and faculty members via the GroupMail/Bulk Mail Distribution Service (BMDS). The CIRC will be responsible for making this decision.	
2.5.3 Activate telephone calling lists and phone trees. The CC is responsible for contacting the persons listed in the roles listed below. They may enlist support from the Help Desk to expedite the work. The CIRC should set priorities, based upon the incident type, and confirm that the task is completed. • ITS Senior Tech Staff (includes the ITS Helpdesk) • ITS Senior Management Staff • UT Executive Offices (and respective technical support staff) • IT Governance Chairs • Other Offices (and respective technical support staff)	
2.5.4 Notices on UT voice mail system. If warranted, have a notice posted on the voice mail system. Contact the SmartVoice Administrator at 471-8820 for assistance. If they are out, press "0" for the operator. Messages on the voice mail system should be kept as brief as possible and prefaced with "This is an official announcement from Voice Mail Administration and ITS".	
2.5.5 FAX transmissions. The CC is responsible for sending notices and updates to the offices referenced above in the event that web services are unavailable for an extended period of time. The LIH should determine the content and the CIRC should approve it prior to	

transmission.	
2.5.6 Posting signs. The CC is responsible for preparing warning signs to be posted around campus. The LIH should provide content. The ITS Helpdesk staff should be advised of any notices which will list them as points of contact. The Remediation Team(s) will be directly responsible for posting this signage once it has been disseminated. The signs should be used: • On doorways to major buildings, departmental offices, and computer facilities. • On attacked computers	
2.5.7 Notification in person or by alternative means. In the event that all networks and telephone services are unavailable or the responsible parties are unavailable by e-mail, phone, or FAX the CIRC will need to determine if the situation warrants notification of responsible parties by runners through either oral or written messages. Any other alternative means of communication, consider for example: engaging the emergency alert siren, lighting the UT Tower in a pre-established, distinctive pattern, using 2-way radios, sounding classroom/building bells, megaphones, etc.	
2.6 Conduct training sessions. The CIRC should ensure that the CIRT has everything needed to begin conducting training sessions on the identification, containment, and removal or eradication of the attack at the earliest opportunity in the training room reserved by the CC. Staff from the ITS Helpdesk should be included in the training sessions.	
2.7 Take the necessary steps to contain the incident and prevent further propagation. On the advice of the CIRT, the CIRC will need to determine if any other actions are required to prevent the situation from getting progressively worse. Whenever appropriate, the CIRC should try to maintain services in accordance with the established list of critical campus servers.	
2.8 The CIRC should determine if Data Breach Notification Plan should be activated (i.e., if protected personally identifiable data has been exposed).	

3. Eradication and Recovery.

3.1 Coordinate Response. The CIRC will assist to organize and contact the incident response teams, make certain that they have the resources needed (hardware, software, media, current patches or updates, etc). The LIH should provide training, if necessary. The CIRT should work with the Remediation Teams to assist department users who have been adversely affected by the incident.	
3.2 Ensure system integrity. Maintain user data. The CIRC should verify that the LIH is continuing to monitor vendor sites, posting material as it becomes available and updating the ITS Helpdesk staff regularly.	
3.3 Determine root cause of incident.	
3.4 Improve defenses: patch vulnerable applications, implement local firewalls/filters. Consider migrating machine's function to a more secure operating system, if warranted.	
3.5 Perform security assessments on systems/networks.	
3.6 Remove the cause and correct any changes it has made and disable or secure any exploitable active services. The Remediation Teams should, based on the training provided by the CIRT work in cooperation with ITS, ITS contract sites, UT Executive offices, and other departments that have been adversely affected.	
3.7 Restore operating system as necessary. If the incident has resulted in damage to the operating system, the Remediation Teams may be called upon to perform a fresh install of the OS. Before doing so, the Remediation Team members should: • Verify that the user data on the system has been backed up. • Confirm the necessity of this step with the CIRT, if necessary. • In the event of a shortage of staff resources, the Remediation Teams may need to set priorities and should and decisions to delay a re-install should be done with the approval of the user. Damaged or attacked systems must be taken off-line until they are remediated. • Clear the re-install with the user or in the case of shared machines, the department contacts.	
3.8 Install service packs, Hotfixes, or security patches as necessary and recommended by vendor. Emergency software updates will be available via UTnet quarantine networks as necessary.	
3.9 Restore user data from backups as necessary. The Remediation Teams are responsible for this task.	
3.10 Bring systems back online. The Remediation Teams are responsible for this task.	
3.11 Change all passwords. All systems must have their administrative passwords changed.	
3.12 Monitor system performance and report activities. Submit a simple report of actions taken and time required to Information Security Office, abuse@utexas.edu, so that pertinent incident information may be filed with the Department of Information Resources (DIR). The Remediation Teams are responsible for this task.	

4. Follow-up.

4.1 Conduct a post-mortem meeting. The CIRT should meet to review its response to the emergency. Topics of discussion should include: • How it happened. • What can be done in the future to prevent similar problems? • How effective the team's initial response was in containing it. • Whether any part of the Incident Management Procedures needs to be improved. • Other lessons learned about UT's ability to respond.	
4.2 Produce the follow-up report. The CIRT should prepare an executive summary of the findings of the post-mortem meeting. The report should include data on the impact of the emergency and recommendations for changes that would minimize or prevent future recurrences of similar problems. An overall incident cost analysis should be included, which would be calculated using the Information Security Office's Incident Database. The CIRC should gather all pertinent incident information so that the Information Security Office may file a formal report with the Department of Information Resources (DIR).	