



UCit Information Security Plan

V 3.1 February 2008

UC Information Security

I. The UC Approach to Information Security Management

University of Cincinnati (UC) is responsible for taking all reasonable and appropriate steps for the protection of the confidentiality, availability, privacy, and integrity of information in its custody, whether in electronic or material form. This includes the physical security of the equipment where information is processed and maintained and the preservation of information in case of intentional, or accidental loss due to natural disaster. In addition, UC is responsible for the maintenance and currency of applications that use this information.

A. Scope of this document

This Information Security Plan applies to all digital and other information whether it is located in computer files, paper files, equipment, or other hard assets where information is stored. Localities and boundaries covered include anywhere UC data is being accessed from and anywhere UC data is being stored.

The plan will define overlapping responsibilities of UCit organizational units and the intersecting responsibilities of other organizations including, but not limited to, consultants and contracted service providers.

B. Guiding principles

UCit Information Security Plan is guided by the principles of business continuity, privacy of student and employee records, risk analysis and management, compliance, education, clearly defined roles and responsibilities, and on-going assessment. Some of which can be found in the Gartner report on best practices attached as Appendix B.

- 1) The emphasis is on *business continuity*, i.e., the *availability* of computing and other resources necessary to carry on the mission of the University.
- 2) The University protects the *privacy of student and employee records* by ensuring the security and protection of confidential information in its custody, whether in electronic, paper, or other forms.
- 3) *Risk analysis and management* is a necessary part of protecting the privacy and confidentiality of information systems. Risk is a fact of life for any organization that must maintain the confidentiality of collected data, whether it is online or consists of paper files. Risk management must include analysis to avoid unnecessary efforts and expenses.
- 4) The continuing *education* of the staff, faculty, and students on security issues is a large part of information security in a University. In addition, as the University develops policies and standards for protecting the confidentiality of sensitive information, employees who handle this data are appropriately trained on these policies and their procedures.
- 5) *Clearly defined roles and responsibilities* assure that the security infrastructure functions as planned especially in a milieu of overlapping responsibilities that occurs in a University.
- 6) *Ongoing assessment* is necessary in an environment of new and evolving threats, new and evolving technology, developing user requirements, and fluctuating economic conditions.
- 7) *Classification of Data*. Information resources are considered to be assets of the University. They are classified according to the risks associated with the data

being stored or processed. Data with the highest risk needs the greatest amount of protection to prevent compromise; data at lower risk can be given proportionately less protection. This approach allows UC InfoSec to apply more appropriate levels of resources to the protection of the assets based upon need.

Example of Restricted Data

Legal Requirements	Reputation Risk	Other Institutional Risk	Access	Examples
Protection of data is required by law (e.g., see list of specific HIPAA, GLB and FERPA data elements)	High	Information which provides access to resources, physical or virtual	Only those individuals designated with approved access and signed non-disclosure agreements	<ul style="list-style-type: none"> • Medical Students • Prospective students • Personnel Donor or prospect • Financial Contracts • Physical plant detail • Credit card numbers • Hazardous chemical location and inventory • Certain management information

C. Definitions of terms in this document

- **Attacks** are actions taken by an entity that exploit certain vulnerabilities.
- **Availability** is a property that assures that the system has the capacity to meet service needs. It includes timeliness and usability. The property of availability protects against threats of denial of service.
- **Controls** are mechanisms or procedures that mitigate threats. Among the goals of security controls are to provide confidentiality, integrity, availability to a computer system.
- **Confidentiality** is a property that assures the assets of a computer system are accessible only by authorized parties or entities. The property of confidentiality protects a system from the threat of disclosure. A disclosure threat is the possibility that data will be accessed by unauthorized entities.
- **Consultants** are experts hired by the university to provide assistance with its information systems.
- **Contracted service providers** are third parties including businesses that are hired by the University to provide assistance with the information systems infrastructure.
- **Integrity** is a property that assures that unauthorized changes in data cannot occur or can be detected if they do occur. The property of integrity protects against threats of modification and fabrication.
- **Privacy** is a subset of confidentiality. It concerns data about a regulated entity and assures that this data is not made public or is accessible by unauthorized individuals.
- **Risk analysis** is the study of the consequences involved in doing something or not doing it. It improves the basis for security related decisions and is based on business needs and cost analysis.
- **Threats** are potential occurrences, malicious or otherwise, that can have undesirable effects on assets or resources associated with computer systems.
- **Vulnerabilities** are characteristics of computer systems that make it possible for a threat to potentially occur. They are not necessarily weaknesses in a system and may be otherwise desirable qualities of a system.

D. Roles and Responsibilities

UCit assumes a *coordinated approach* to the protection of information resources and depositories of confidential information that are under its custody by establishing appropriate and reasonable administrative, technical and physical safeguards that include all individuals, related units, or others that administer, install, maintain, or make use of UCit's computing resources and other depositories of information. The Office of VP for IT and CIO provides leadership for the University's Information Security environment and the Director of Information Security will be responsible for establishing strategic direction as well as the development, maintenance, and yearly review of the IS Plan, in collaboration with units under the supervision of the following managers:

- Chief Information Officer (CIO)
- Director of Network and Telecom Services
- Director of System Operations
- Director of Educational Technologies
- Director of Internal Audit

II. Driving Factors for On-going Security Planning

A. Risk Assessment

The risk assessment includes, at a minimum, the following elements:

1. An inventory of information assets in the business environment
2. A determination of the security needs of the university computers and networks
3. An evaluation of the management and control of security risk including:
 - a. Risk assessment
 - b. Mitigation of risk
 - c. Vulnerability assessment
4. Creation of policies and procedures for the life-cycle management of secure information assets (including confidential information)
5. Staff orientation and training

B. Compliance with Legal Requirements

A key goal of this plan is to assure that UC is in compliance with Local, State, and Federal laws and regulations including but not limited to:

1. Gramm-Leach-Bliley Act

Summary

GLB requirements mandate the design, implementation, and maintenance of specific policies to protect customer information.

GLB protects consumers' personal financial information held by financial institutions. It contains two major sections:

- 1) The maintenance of privacy for customer and consumer information, and
- 2) The safeguarding of consumer and customer information

Responsible Department

Finance CFO/ Treasurer

2. Federal Trade Commission Regulations (16 CFR, Part 314), Standards for Safeguarding Customer Information; Final Rule, May 23, 2002

Summary

Implements the Safeguarding provisions of the Gramm-Leach-Bliley Act.

Establishes standards for safeguarding customer information and creates a method to guarantee the uniform application of these standards (Information Security Program)

Creates a list of tasks to develop, implement and maintain the Information Security Program.

Our Responsibilities

Develop, implement and maintain a University wide Information Security Program

Responsible Department

UC Information Security

3. Family Educational Rights and Privacy Act (FERPA)(20 U.S.C. S1232g; 34 CFR Part 99)

Summary

Protect the privacy of student education records
Gives Parents certain rights with respect to their children's education records

Our Responsibilities

Schools may not disclose information without consent
Schools must give parents access to records
Schools must allow parents to request that inaccurate records be corrected

Responsible Department

UC Registrar

4. HIPAA (Health Insurance Portability and Accountability Act)

Summary

These regulations specify what patient information must be kept private; how companies must secure the information; and the standards for electronic communication between medical providers and insurance companies.

Our Responsibilities:

Help our Affiliates protect all PHI and EPHI following the guidelines outlined in the HIPAA rules

Responsible Department

UC Information Security

5. Payment Card Industry (PCI)

Summary

The PCI Data Security Policy requires that all PCI Data Security Members, merchants, and service providers that store, process or transmit cardholder data verify all purchased and custom web applications, including internal and external (web) applications.

Our Responsibilities

Protect cardholder data by following the 12 Payment Card Industry (PCI) Data Security Standard (DSS) requirements.

Responsible Department

UC Finance CFO/Treasurer

III. Policy development and Management

A. University Information Security Policies and Procedures

The University is developing a body of information security policies and procedures for the protection of the business infrastructure and environment, the computing infrastructure and environment, and the confidential information in its custody.

B. Managing Compliance with University Policies

- 1) Monitoring compliance and violations of policies and procedures
- 2) Enforcement – Response to breaches of policy and procedures involves all that may be involved.

- a) Faculty
- b) Administration
- c) Bargaining units
- d) Student Affairs
- 3) Continuing assessment of policies, monitoring procedures, and enforcement
- 4) The Director of Information Security is responsible for the management of the Information Security Policies at UC.
- 5) The Director of Internal Audit is responsible for auditing against the IT and Information Security policies at UC.

C. Status of Current Policy Initiatives

The following policies have gone through the ratification process and approved. They are published on the UCit Web site.

- 1) *Student E-Mail Policy*
- 2) *Information Technology Management Policy*
- 3) *Network Connection Policy*
- 4) *Perimeter Firewall Policy*
- 5) *Use of Information Technology*
- 6) *Domain Name System Policy*
- 7) *Internal Mass Communications Policy*
- 8) *Retired Equipment Cleaning Process Policy*
- 9) *Wireless Communication Policy (Guidelines on managing air space)*

The following are proposed policies and they can be found on the UC Information Security Web site:

- 1) *Umbrella Information Security Policy*
- 2) *Security Awareness Policy*
- 3) *Password Policy*
- 4) *Cryptography and PKI Policy*
- 5) *Information Security Forensic Investigation Policy*
- 6) *Cyber Security Emergency Response Policy*
- 7) *InfoSec Clean Desk Policy*
- 8) *UC InfoSec Security Records Policy*
- 9) *UC HIPAA Policy*
- 10) *UC InfoSec Data Classification Guidelines*

IV. Operational Management

A. Common Approaches

1) **Managing compromises or breaches of Information security – Incident Response Team** (see Appendix A)

Planning for incident management involves organizing an Information Security Incident Response Team that is responsible for *problem identification and resolution*. This team has clearly defined membership, roles, and responsibilities. The issues an Incident Response Team is concerned with include (but are not limited to):

- a) Business decisions
- b) Existing and evolving threats
- c) Ongoing problems
 - a. How to monitor them

- b. Solutions
- d) Policies
- e) Security Testing
- f) Incident Management
 - a. How to trigger a response
 - b. Automated and manual responses
 - c. Reporting responsibilities
 - d. Certification of actions
 - e. Post-Mortem review and recommendations

2. Oversight of vendors, consultants, and contracted service providers

UCit will require consultants and other service providers that are permitted access to confidential data to provide adequate safeguards. When applicable, contracts with such service providers will include the following elements regarding data security:

- a) Explicit acknowledgement that the contract permits the contractor to have access to confidential information
- b) A definition of the confidential information to which access is granted
- c) A stipulation that the confidential information must be held in confidence and accessed and used only for the explicit business purpose specified in the contract
- d) A stipulation from the contractor that it will ensure compliance with the protective conditions specified in the contract
- e) A provision requiring the contractor to return and/or destroy all copies of confidential information upon completion or termination of the contract
- f) A stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles the University to immediately terminate the contract without penalty
- g) A provision in the contract that holds the University harmless for disclosure or misuse of confidential information.
- h) A provision allowing an annual audit of the contractor's compliance with protective conditions.
- i) A provision ensuring that the contract's protective requirements shall survive any termination agreement.

3. Ongoing Assessments and Improvements by UC Internal Audit

- a) Plans for continuous assessment and improvement
 - a. Evaluation
 - b. Adjustment
- b) Policies for assessment
- c) Inclusion of entire University Community in assessment and improvement cycle
- d) Internal and External assessments

4. Policy for Managing Confidentiality/Privacy

B. Business Environment

1) Protecting the Information Security Assets of UCit

- a) Academic
- b) Administration
- c) Students
- d) University Advancement
- e) University Corporation
- f) Auxiliary and Extended University

2) Business Continuity Planning for the Business Environment and Information Security Emergency Response planning

The specific elements of this program is:

- a) Active integration and collaboration with the Emergency Operations Center teams. (See appendix A for details)
- b) Development of ISERT Plans for all key functional areas.
- c) Development of ISERT tools to support Business Continuity efforts.
- d) Facilitation and support of ISERT to ensure that effective and integrated solutions are created.
- e) Ongoing testing of all key functional areas.

C. Infrastructure Environment

1) Securing the University Computing Infrastructure

The Director of Information Security (DIS) is responsible for the management of threats on an ongoing basis. Thus the DIS's operational duties include:

- a) Keeping current with security study and examination
- b) Establish Strategic Direction in the area of InfoSec for UC
- c) Security planning for more stability and decreased complexity of the information infrastructure
- d) Overseeing standards and regulations (guidelines and policies)
- e) Risk Analysis and Management
 - 1. Costs vs. Performance
 - 2. Risk Review and Acceptance
 - 3. UC uses the following two risk management concepts to as a guide when making infrastructure decisions:
 - a. The Principle of *Least Privilege*: Anything that is not expressly permitted is denied.
 - b. The Principle of *Need To Know*: Information is compartmentalized and only those who need that information have access to it.
- f) Identifying key weaknesses in the Infrastructure
 - 1. Liability Issues
 - 2. Audit findings
 - 3. Hodgepodge of pieced together systems and methodologies stemming from the history of the development of IT at the University:
 - a. Fragmented organization
 - b. Informal and de-facto policies

2. Business Continuity Planning for the Infrastructure Environment

Infrastructure and Server Operations management uses three documents to support business continuity:

- a) Disaster Recovery Instructions
- b) Strategic and Tactical Plans for Disaster Recovery
- c) Testing Documentation

3. Specific Infrastructure Security Procedures by Area:

A) Networking Environment (data, video, and voice)

The primary InfoSec concerns at UCit for NTS are in the areas of denial of service, copyright violation, unauthorized use of resources, traffic anomalies, privacy/confidentiality, and protection of physical assets.

The following technologies and tools supported by the appropriate policies and procedures are implemented to address these needs:

- Wireless WEP/WPA2
- Firewalls
- Intrusion detection and Intrusion Prevention
- Access control lists
- Virtual Private Network
- Authentication/Authorization
- Port limitation (restrict MAC/port)
- Physical Access controls
- Endpoint Security (ResNet)

B) Enterprise Serving Environment

Management of the serving facility protects the enterprise servers from unauthorized access, DOS attacks, and email threats, (virus, Trojan, backdoor, worms).

Operational procedures allow access to only authorized users by ensuring that they securely log on, authenticate, and have access appropriate to their job roles.

C) Middleware Environment

Highly Restricted data (defined by State/Federal laws and regulations) must be encrypted over un-trusted networks.

The minimum amount of access is allowed to achieve goals.

- Servers
 - Only necessary ports are open
 - Local firewall configured to allow access to only a minimum set of necessary hosts
 - Only necessary services are run
 - Only necessary access is allowed.
- Applications
 - Only the minimum set of privileges allowed for user to accomplish his/her objective

Unusual account access (ex: named accounts with enriched privileges, network access) are not available through the directory.

Passwords are designed with the required complexity and changed every ninety days.

D) Desktop Environment

UC InfoSec will provide consulting for UC staff, students and affiliates in the area of protecting their desktop. In certain areas (ResNet) tools such as CISCO clean access will be used to insure that a baseline of security is maintained across desktop systems that touch the UC infrastructure.

E) Application Development Environment

Security falls into two areas:

1. Authentication
2. Authorization

User authorization to applications is at the discretion of the functional end user departments.

Transactions, both inquiry and update, are performed using Screens. The access to individual screens, together with the actions that can be performed, are assembled into one (or more) "Permission List" by the management and security personnel in each functional end user department.

Permission lists are, in turn, assembled in one (or more) "Role" by the management and security personnel in each functional end user department.

One (or more) Role is assigned to each individual by the Help Desk, after approval is received from the manager of the functional end user department.

All access privileges applications are at the sole discretion of the management of the functional end user department. No other access to the applications or databases is granted to UC IT personnel, except those engaged in Database and System Administration support activities.

F. Specific Security Issues Which Span Organizational Boundaries

- 1) Management of Spam
- 2) Management of Denial of Service Attack
- 3) Copyright Infringement
- 4) Confidentiality and Privacy
- 5) Maintenance of a non-hostile work environment
- 6) Various Investigations
- 7) Regulatory and Research Compliance

V. Employee Education and Training

The entire University Community needs to understand and support the information security objectives of Confidentiality, Integrity and Availability (CIA) and what tradeoffs may be necessary for effective control of the information infrastructure's vulnerabilities. The University has begun to implement a plan of security education throughout the enterprise that will include a consultative process that informs as well as receives input:

- Staff and faculty orientation and training
- Student orientation
- Administrative Councils
- Other auxiliary and enterprise fund units

A. Employee Training

The University has policies and standards that coordinate procedures for preserving the security of data. Each unit identified as receiving, holding, or using such data, whether in electronic form or in paper documents, is required to restrict access to and control usage of the data.

The responsible person ensures that each area has such controls in place that conform to the University policies governing confidential data, and that employees who handle covered data are both appropriately trained and adequately supervised. Such training includes education on relevant policies and procedures, and other safeguards designed to protect data.

Other safeguards that are applied when appropriate are:

- 1) Limiting access to confidential data on a need to know basis,
- 2) Requiring signed certificates of responsibility prior to authorizing access to the covered data, and
- 3) Requiring signed releases for disclosure of covered data.

B. Training on Security Related Policies and Procedures

Policies and procedures are posted on the University Web page to facilitate their communication throughout the enterprise. The University facilitates employee compliance with all security policies through:

- 1) A plan of education on these policies.
- 2) Requiring signed certificates of knowledge of each policy

VI. Management of the Information Security Plan

Oversight and management of the campus' Information Security Plan will be the responsibility of the UC Director of Information Security.

Operationally, the actual development, testing, and deployment of planning elements will be managed by the UC Information Security Office in collaboration with the UC Internal Audit team and UC IT Coordinators from UC units.

University of Cincinnati

Information Security Emergency Response Plan

Department of Information Security

Version 0.1



University of Cincinnati

Information Security Emergency Response Plan

Department of Information Security

Version 0.1, Draft

Table of Contents

Information Security Emergency Response Plan Charter	17
Information Security Emergency Response Information Flow.....	18
Information Security Emergency Response Plan Services	19
Emergency Response Guidelines for CIO/ DCIO/ Leadership Team.....	25
Information Security Emergency Response Team Roles and Responsibilities	26
Priorities in Emergency Handling	34
ISERT Example Emergency	35
Determining that an Emergency is Critical: Emergency Severity Levels	35
Team Makeup by Position Title.....	39
Appendix A – Information Security Emergency Review Report.....	40
Appendix B – Who Contacts Whom	42
Appendix C – Time Guidelines.....	43
Appendix D – Tabular Summary of Data Valuation.....	44
Appendix E – Tactical Organization Equipment list.....	45
Appendix F – Forensic Evidence Methodology	48
Appendix G – UCit Disaster Recovery Plan.....	51
Appendix H – Order of Succession for CIO Duties.....	52

Proprietary

This document is the Confidential & Proprietary property of the University of Cincinnati. Do not distribute outside of the University of Cincinnati without prior written consent from the Director of Information Security.

Kevin L. McLaughlin

Suite 400, University Hall
51 Goodman Drive
Cincinnati, OH 45221-0149
(513) 556-9177
infosec@uc.edu

Information Security Emergency Response Plan Charter

Information Security Emergency Response Plan

Purpose

The purpose of this Information Security Emergency Response Plan (ISERP) is to provide the University of Cincinnati with a plan that addresses the dynamics of an information security emergency. An information security emergency is one that threatens confidentiality, integrity or availability of the University of Cincinnati information assets with high impact, high threat involving high risk and great vulnerability. The ISERP defines the roles and responsibilities for Information Security Emergency Response Team (ISERT) members, defines emergency severity levels, outlines a process flow for emergency management, and includes methodologies for conducting response activities.

The ISERT may be initiated by itself or in cooperation with other emergency response plans during certain disasters declared at the University of Cincinnati. For example, a situation in which the UC Disaster Recover or Business Continuity Plans (DR/BC) is activated may also require the activation of the ISERT.

Should the ISERT be activated as part of a wider University Disaster, all activities in this plan (The ISERP) will be subject to the authority and direction of the CIO, unless specific authority is given to the DR/BC team by the CIO in writing.

The following table summarizes these relationships:

Activity	Managed By	Document
Emergency Response (Service Disruption)	Appropriate UCit Groups	
Information Security Emergency Response	CIO	Information Security Emergency Response Plan
University Disaster	DR/BC Coordinator	The UC Disaster Recover / Business Continuity Plans

Scope

The ISERP applies to the University of Cincinnati's Information Technology Services and all systems and services for which it is responsible.

This ISERP covers all computer systems and networks connected to The University of Cincinnati's network, to include the campuses in Clermont and Raymond Walters College. The ISERP is mandated to take all actions required to assure the protection of The University of Cincinnati's reputation, information assets and the student, faculties, and staff information assets that reside under The University of Cincinnati's control.

Under some circumstances the ISERP should be used for servers and systems used by other departments within the University.

Definitions and Acronyms

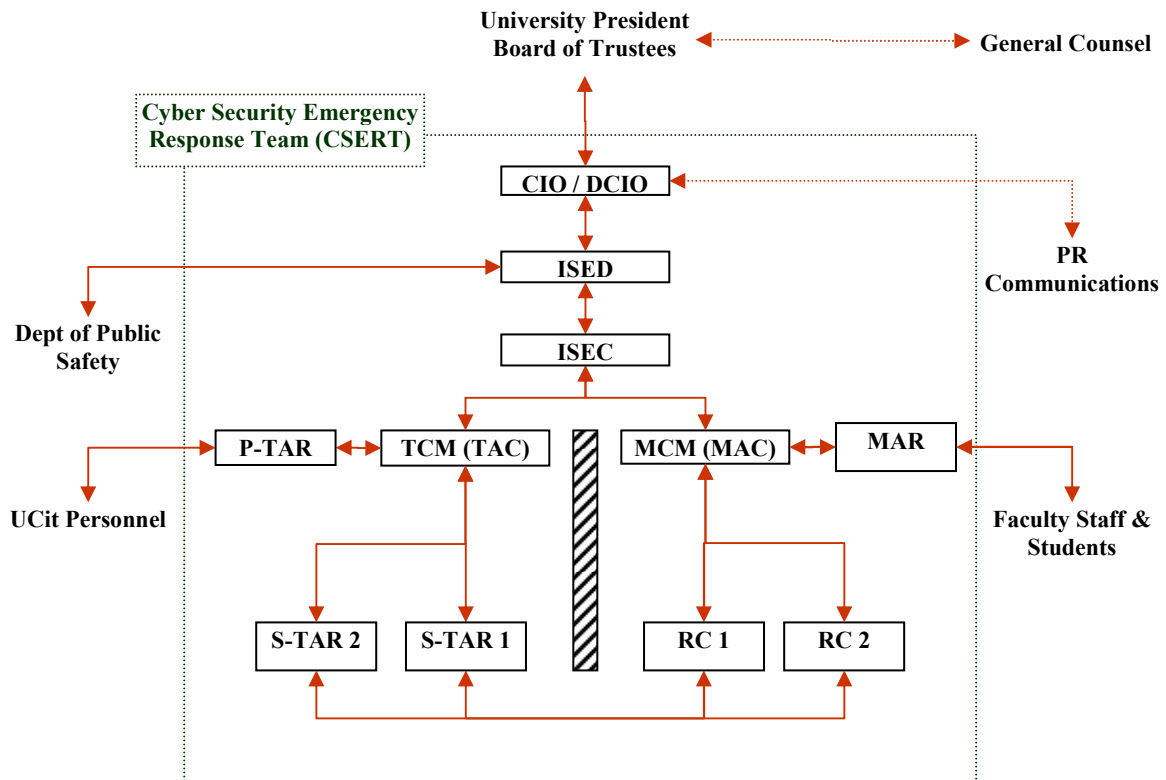
- ISERP – Information Security Emergency Response Plan
- ISERT – Information Security Emergency Response Team
- SED – Information Security Emergency Director(s)
- TCM – Technical Communications Manager

- TAR – Technical Alert Roster
- TAC – Technical Audio Conference
- MCM – Management Communication Manager
- MAR – Management Alert Roster
- MAC – Management Audio Conference
- RC – Resource Coordinator
- Information Security Emergency – See the table of contents for a whole section defining Information Security Emergency

Policy for UCit

Information security emergencies will occur that require full participation of IT technical personnel as well as college or departmental leadership to properly manage the outcome. To accomplish this, the Office of the Chief Information Officer will establish information security emergency response procedures that will ensure that appropriate leadership and technical resources are involved to (1) assess the seriousness of an emergency, (2) assess the extent of damage, (3) identify the vulnerability created and (4) estimate what additional resources are required to mitigate the emergency. It will also ensure that proper follow-up reporting occurs and procedures adjusted so that responses to future emergencies are improved.

Information Security Emergency Response Information Flow



The above diagram illustrates how information regarding the nature and management of an information security emergency should be communicated. The ISERT may become aware of a suspected information security emergency in a number of ways. Some examples include:

- An intrusion detection (IDS) sensor reports suspicious network traffic
- The log files on the firewall show a large volume of “denied” packets from several Internet sites, with patterns suggesting a determined attempt to gain access
- A user reports, through the Support Desk or other means, that their system appears to have been infected by a computer virus or other malicious agent
- Media reports suggest that a fast-spreading computer virus/worm has been discovered, causing widespread shutdowns of corporate electronic mail systems
- University Communications and/or Risk Management receive a telephone call from a reporter seeking comment on another site’s claims that The University of Cincinnati’s systems were used to break into the caller’s systems

Regardless of how the information security emergency alert reaches The University of Cincinnati, an ISEC must be identified and notified in the most expeditious manner to ensure appropriate action (see steps in the Alert phase below). During normal business hours the alert may come from the Support Desk; whereas after hours the alert may be generated by the Data Center personnel.

Information Security Emergency Response Plan Services

This plan’s main function is to assist with the response and management of an information security emergency. This ISERP will provide information on two types of services that contain emergencies and protect The University of Cincinnati’s reputation. The two primary ISERP services are proactive services and reactive services and they are described within this section. It is important to understand that this document is a “living” document and routine maintenance is necessary to ensure that the information within it is accurate and current. The Security Office is responsible to see that the Information Security Emergency Response Plan and related policies and procedures are maintained, distributed to team members, and communicated to upper management. The Help Desk is responsible to keep contact information current.

Proactive Services

Proactive Services are ISERT tasks designed to prevent or mitigate the severity of an emergency before it occurs. These services are provided when the team is not actively managing an emergency, and include: Plan Maintenance, Policy Changes, Plan Education, Announcements, Plan Testing, and Setup & Maintenance of resources required to function during and extended emergency.

<u>Education</u>	<ul style="list-style-type: none"> • Provide necessary training to people concerning their roles and responsibilities as identified in the plan • Provide ISERT awareness training to UC community
<u>Plan Testing</u>	<ul style="list-style-type: none"> • Perform semi-annual plan tests and coordinate the remediation of identified issues
<u>Maintenance</u>	<ul style="list-style-type: none"> • Maintain the ISERP according to standards established by CERT command center. • Update the ISERP based on lessons learned from post-mortem review, and update contact information as members change • Schedule regular testing procedures to ensure information is correct and the information flow is clear to the named ISERT members
<u>Resources</u>	<ul style="list-style-type: none"> • Obtain required resources (should we detail?) • Check resources semi-annually. Remediate any issues found

Preparation steps

Main Idea: create an infrastructure that provides rapid answers to questions that you will have after an emergency occurs.

1. Identify your vital assets.
2. Prepare individual hosts
3. Prepare the network
4. Establish appropriate policies and procedures
5. Create a response tool kit
6. Establish an emergency response team

Reactive Services (Response Steps 2 thru 6)

Reactive Services are broken into five (5) categories; Notification, Triage, Response, Recovery, and Maintenance.

<u>Notification Phase</u>	During the Notification phase, the initial emergency report is generated and reported to the ISED. Once the report is received, the ISED makes a preliminary escalation determination based upon suspected or confirmed elements of the alert.
----------------------------------	--

2.0 Detection and Analysis — Begin Notification Phase

2.1 Emergency is suspected to be critical

2.1.1 Reports of emergencies without classification are received by UC personnel from a variety of sources. For example: abuse@uc.edu, infosec@uc.edu, helpdesk, IT Coordinator List Serve, UCit Management. The UC InfoSec team monitors these sources.

2.1.3 Emergency is suspected to be an Information Security Emergency? No = proceed. Yes = go to 2.2

- See the definition of information security emergency in this document (page 14)

- See examples of information security emergency in this document (page 15)
- Consider the following. Has confidential data been exposed? Could it involve violation of the law? Could it involve notification of customers? Have critical services been disrupted for an unacceptable length of time?
- See Appendix D summarizing data valuation

2.1.4 Staff assigned by Support Services or the NOC to evaluate non-information security emergencies. The result may be that the emergency is suspected to be critical.

2.1.5 Emergency is suspected to be an Information Security Emergency after further investigation? No = resolution Yes = go to 2.2

Triage Phase	Whether an emergency is actually critical is assessed by the ISED during Triage phase. It may or may not be declared a Information Security Emergency; if determined to be an emergency, the ISERT is assembled and resources are assigned.
---------------------	---

2.2 Suspicion of a Information Security Emergency is reported to ISED. ISED notifies support resources that the ISED is monitoring the incident.

2.2.1 Suspicion of a Information Security Emergency should be logged with the time stamp and relevant factors that raised the suspicion. Mandia p. 19

2.2.2 How long after report of suspecting that an emergency is critical does the Help Desk have to contact and/or get ownership by a coordinator? Generally 10 minutes. Note that in other cases the help desk has procedures to get a person on the job in 10 min. The answer should take into consideration how long the ISEC has to respond to the call.

2.2.3 Assess the extent of the damage, identify the vulnerability created, and estimate what additional resources are required to mitigate the emergency.

2.3 Declaration of Emergency: If situation is deemed by ISED as possible emergency, ISED contacts the CIO recommending that an Information Security Emergency be declared. If CIO is unavailable, ISED become DCIO for the purposes of the emergency response and coordination. An oral statement by the CIO constitutes a declaration.

2.3.1 See page 13 for the ways that an emergency may be declared critical

2.3.2 See section 2.1.3 for ways to distinguish a critical from a non-information security emergency

2.3.3 Information Security Emergency Declaration is issued? No = goto 2.1.x. Yes = proceed.

2.3.6 How is a declaration recorded? The ISED will record in the ISERT log book the fact that the emergency has been declared critical & by marking the 'Emergency Report' form. The ISEC should also make a written log entry with date/time stamp and the factors that made the emergency critical.

- ISED and ISEC Checklists are obtained and distributed to ISED and ISEC.

2.3.7 Notification checklist is completed? The ISEC should log the fact that all required notifications are complete.

2.3.9 How is a information security emergency downgraded? A Information Security Emergency may be downgraded at any time by simple agreement of the CIO. Any time the ISED concludes that the emergency does not in fact meet the conditions of a information security emergency, they should get agreement from the Sr Director who is assisting the emergency and take a written request to downgrade accompanied by the reasons to the CIO for signature. The CIO

should respond as quickly as possible. Timely response from the CIO is important because resources will continue to be consumed to treat the emergency as critical until it is downgraded.

Response Phase	The Response phase includes developing the plan to provide analysis and containment of compromised systems and elimination of the emergency's source. The ISEC will assign response plan tasks to specific members of the ISERT.
-----------------------	--

Response

- The ISERT will identify the cause of the information security emergency
- The ISERT will fully determine the containment process and determine which actions are immediately required to minimize any additional loss and/or exposure to information assets
- During the response phase the first responder(s) need to be familiar and comfortable with the evidence collection guidelines. Every emergency is handled differently, however, strong documentation will assist with protecting the evidence and ensuring the Chain of Custody is intact. (See Appendix F)

2.4 Information Security Emergency Response Team is assembled—Begin Response Phase

2.4.1 The ISEC identifies team members and uses whatever resources required to contact team members and draft them to be part of the team. Membership on the team will vary according to the nature of the emergency. At minimum you will have an ISEC, a scribe, and a technical person. The ISEC could act as the scribe if the time permits. Team members may negotiate with the ISEC on whether to serve but ultimately must report if the ISEC requests it. Any UCit employee may be drafted to the team although the preference is to select from the list of technical staff in this document (page 23).

2.4.2 The coordinator formulates initial response

2.5 Initial Response

2.5.1 Any emergency measures not already taken to deliver initial containment and perform deeper analysis of the event.

2.5.2 Is it really a Information Security Emergency? No= goto 2.1.x. Yes = proceed

2.6 Formulate Response Strategy. (Mandia, p. 21)

2.7 Present Response Strategy Options to Management. The ISEC will attempt to get management input but may proceed without it.

3.0 Containment and Investigation

3.1 Containment and investigation may be pursued simultaneously. Containment means prevent the spread of a problem from A to B. Containment could occur in the NOC before a information security emergency is declared.

3.2 Secure the system, secure means prevent the problem from getting to A again. (Mandia p. 26)

3.5 Monitor affected systems. (Mandia p. 27)

3.4 Investigate Cause. (Mandia p. 25)

3.6 Isolation specific issue.

4.0 Eradication

4.1 Eradication may be necessary to eliminate components of the emergency such as deleting malicious code or disabling breached user accounts.

4.2 For some emergencies, eradication is either not necessary or performed during recovery.

Recovery Phase	During the Recovery Phase, the ISERT investigates the causes for the emergency and assesses the damage incurred. Affected systems and services are restored to their original state. The ISERT conducts post mortem activities to identify and document the root cause and business impact of the emergency and remediation activities required to prevent its reoccurrence.
-----------------------	--

Recovery

- Implement actions determined during the response phase as required to recover affected systems. Production systems that do not require configuration changes are then returned to their original state
- In addition, systems that require configuration or application changes to prevent the emergency's reoccurrence are updated, tested, and redeployed into production.

5.0 Recovery—Begin Recovery Phase

5.1 Consider what was compromised

5.2 Choose a recovery strategy. The following is a suggestive list: ghost, patch, code upgrade, application fix, firewall rule, quarantine, packet shaper filters, access control list, intermediate recovery on alternate equipment.

5.2.1 Intermediate recovery on alternate equipment may involve pre-arranged agreements with alternate sites such as: The Ohio State University or Miami University. **The Server Operations Team has information on these agreements and the ISEC will need to involve the Server Operations team if they are to be used.** The ISEC should be aware that intermediate recovery to alternate equipment could lengthen the overall recovery time.

5.2.2 **A document titled "Production Disaster Recovery" kept on the Server Operations team sharepoint site contains an up-to-date and comprehensive description of applicable resources and procedures.** A University Disaster does not need to be declared to use many of these resources; a Information Security Emergency Coordinator (SEC) may use resources provisioned in Disaster Recovery when permission is granted by the CIO.

5.3 Recover to normal operations

5.4 Harden systems to prevent similar emergencies

5.5 Declare to the CIO that the emergency is resolved and transfer control of the relevant services back their respective owners. The emergency is not finally closed until the completion of the next phase, phase 6.

End Phase	Ongoing validation of the Information Security Emergency Response Plan and the ISERT process will be achieved through regular exercises and after action reviews in the Maintenance phase.
------------------	--

End Phase

- Post-mortem exercise is conducted to identify root cause and areas of improvement. See report in **Appendix A.**
- This exercise should be conducted within 2 weeks of the emergency.
- Any changes to the ISERP or policies/procedures should be addressed

- After the post-mortem phase is completed the information security emergency can be closed by the ISED.

6.0 Follow-up—Begin End Phase

6.1 Support criminal or civil prosecutions

6.2 File a Information Security Emergency Review Report (**Appendix A**) with the CIO's office and schedule a review meeting. CIO or a designee is to preside.

- Determine Root Cause*
- Determine Root Effect*
- Determine Key Learnings*
- Determine Total Cost of Emergency*
- Publish and close emergency with suggested updates to the Information Security Emergency Response Plan (ISERP)

*The exercise of determining the root cause, root effect and the total cost of an emergency may not occur for each emergency. The CIO will direct the Information Security Emergency Response Team when NOT to perform these tasks.

6.3 Suggest process improvements to the ISED.

Emergency Response Guidelines for CIO/ DCIO/ Leadership Team

2.3.5.1 Receive Declaration of Information Security Emergency From SEC. Ask questions like the following:

- Is it a Information Security Emergency within IT Services?
- Are you declaring a information security emergency?
- Does the NOC know about this and that you are the SEC
- Has data been lost or corrupted
- Do you need anything from me?
- Contact me when you have formulated a strategy or in _____ minutes.

2.3.5.2 Assess the severity of the emergency and determine leadership pattern

- Is it a Information Security Emergency within IT Services?
- Is it a Disaster within IT Services? If so evaluate whether the existing ISEC should be replaced with a coordinator skilled in off site recovery procedures and invoke the off site recovery plan in Appendix H: UCit Disaster Recovery Plan.
- Do I suspect that the emergency is a University Disaster? If so contact Richard Norman and request the he invoke the Business Continuity plan and appoint a University Disaster Coordinator.

2.3.5.3 Decide whether to contact the University counsel and possibly the PEC if the following exist:

- Has confidential or critical information been exposed?
- Has a law been broken? Ask the University counsel to contact campus police
- Could the University have some legal liability from the emergency?

2.3.5.4 Decide what communication plan to invoke within IT Services

- Is this emergency so severe that it requires a gag order. In a gag order, no communication goes out side of UCit even to clients. Remember that until a Information Security Emergency is declared and until a gag order is requested, the support desk will normally discuss outages with clients.
- Does the CIO handle all communication outside of UCit using the Director of University Communication?
- Does the CIO ask the ISEC to use the support center to contact University departments?

2.3.5.2 Begin a personal log of activities for inclusion into the Emergency Report

2.3.5.4 Each time the CIO receives reports from the SEC, consider whether to contact other parts of the organization

- University Counsel who in turn is responsible to contact law enforcement and the FBI
- President and the Presidents Executive Counsel
- University Communications

3.3.1 Decide whether to collect forensic data

5.5 Receive Declaration of Resolution from the SEC

6.0 Receive written report from the ISEC within time frame specified by the CIO

6.0 Meet with the ISEC and other CIR team members to discuss the emergency (generally within one week of the emergency)

Information Security Emergency Response Team Roles and Responsibilities

Within this section, the roles and responsibilities for the CIO, ISED, ISEC, Information Security Emergency Response/Recovery Team (ISERT), and Supporting Groups are defined. In addition, this section addresses the various UCit functional areas within the University of Cincinnati and their ISERT responsibilities.

Chief Information Officer (CIO)

During a disaster, this position will report directly to the University of Cincinnati's President and Board of Trustees. This role will either involve or inform as the needs of the emergency dictate. Communication of information during an emergency will follow this flow to eliminate confusion and misinformation between groups.

The CIO is responsible for executing or delegating the tasks below.

- Set priorities
- Designate the DCIO or an alternate to cover the responsibilities of the CIO role
- Notify the University of Cincinnati President and/or Board of Trustees of a declaration of emergency
- Notify University Communications as appropriate for internal and external communication
- Define and issue 'gag' orders within UCit for particularly sensitive issues; the default guideline for communicating about an information security emergency is on a need to know basis
- Approve requests for external resources over \$10,000
- Notify Human Resources as appropriate
- Notify Legal as appropriate
- Notify Campus Security as appropriate
- Participate with ISED in forensic investigation decisions
- Participating in the Post Mortem

Backup: DCIO

Deputy Chief Information Officer (DCIO)

- When the CIO cannot be reached, the DCIO will fulfill the roles above of the CIO.

Information Security Emergency Director (ISED)

- Maintain communications between ISERT and the CIO
- Advise the ISEC on whether a suspected emergency should go to the CIO for declaration
- Recommend to the CIO, if warranted, that the information security emergency be upgraded to a disaster
- Communicate status of information security emergency to the Public Safety
- Oversee the work of the ISEC during the emergency and report to the CIO as directed.
- Own the ISEC's emergency work plan(s)
- Obtain technical expertise based on the emergency declared (in cooperation with the ISEC and RCs)
- Approve the containment plan provided by the ISEC and TAR

- Approve requests for external resources at \$10,000 or below
- Receive and evaluate the post implementation review report from the ISEC.
- When assigned to do so by the CIO, do any of the tasks on the CIO list
- Conduct training at least annually
- Chair the Post Mortem

Backup: DISED

Deputy Information Security Emergency Director (DISED)

- When the ISED cannot be reached, the DISED will fulfill the roles above of the ISED.

Information Security Emergency Coordinator (ISEC)

This position will update the ISED on a regular basis during a information security emergency. The University of Cincinnati has a backup ISEC. Should the primary ISEC be unavailable or unavailable for a portion of the emergency, then the ISED should call the next ISEC within 10 minutes. Note:

- The ISEC may be asked to run an emergency outside of their functional area.
- If the ISEC is initially unavailable, the alternate will assume the ISEC role in his/her stead.

During a declared emergency, the ISEC is responsible for the following:

- Managing emergency resources
- Determining if an emergency is a Information Security Emergency and requesting formal declaration through ISED
- Communicating to the NOC and the UCit Leadership Team that a information security emergency has been declared and the ISERT has been activated
- Activating the ISERT. Notifying the Technical Communications Coordinator (TCC), Management Communications Coordinator (TCC) and scribe of meeting locations and call-in telephone numbers
- Reminding staff that communication is on a need to know basis or if the CIO has defined a 'gag order' informing team members and the NOC of the nature of the 'gag'
- Coordinating information between the technical and management side via the Technical Communications Coordinator (TCC) and Management Communications Coordinator (TCC)
- Keeping the ISED informed of status and events as warranted
- Obtain technical expertise based on the emergency declared (in cooperation with the ISED and RCs)
- Develop containment procedures in cooperation with TAR (to be approved by ISED prior to implementation)
- Managing the emergency work plan(s) and task assignments
- Raising dependency issues as they arise
- Identifying external personnel/resources as needed
- Designating an alternate ISEC to cover the responsibilities that span more than 12 hours
- Coordinating hand-off meetings between shifts, and developing work plans that address tasks completed and outstanding
- Certifying that all systems are returned to operational quality with the cause rectified
- The secure destruction/retention of all materials at the end of an emergency
- Working closely with the CIO and University Counsel during forensic investigations

- Establishing a Post Mortem Team to determine the root cause and root effect of the emergency

Backup: Backup ISEC

Backup Information Security Emergency Coordinator (Backup ISEC)

- When the ISEC cannot be reached, the backup ISEC will be called to fill the role.

Information Security Emergency Response Team

During an emergency the ISEC will assemble a team. Members will vary depending on the skill sets required to assist during an emergency. Teams will vary in size depending on the need. This team will remain active until the emergency is closed. The members will include staff from UCit as required by the event. This team will be responsible for both response and recovery.

Response:

The response duties of the team are to conduct triage of the emergency, assist in containment of the emergency, collect evidence for the post mortem report and if requested, conduct or assist in a forensic investigation.

- Assisting in the collection of evidence during an emergency investigation
- Making recommendations to the ISEC on remedial action on affected systems
- The Response Team may be called up 24 hours a day, 7 days a week, 365 days a year during a information security emergency

Recovery:

The response aspects of the team are centered around damage assessment, return to normal operations, rebuilding servers and systems, etc.

- Determining whether affected systems can be restored from backup tapes, or must be reinstalled
- Scrubbing all data before making it ready for reinstall
- Determining what data is lost and cannot be recovered or restored
- Reloading data on affected systems
- Restoring normal operations

Technical Communications Coordinator (TCC)

The TCC is responsible for communication and support of the technical people that are solving the problem. Requests for resources should go from the TAR to the TCC.

- Activating appropriate personnel from the Technical Alert Roster (TAR) as directed by the ISEC
- Initiating and monitoring the Technical Audio Conference (TAC)
- Calling the activated TAR members once per hour (and only once per hour) requesting status
- Updating the ISEC hourly or as events warrant

Management Communications Coordinator (MCC)

The MCC is responsible for providing approved status statements to members of UC that call asking for information.

- Alerting appropriate personnel from the Management Alert Roster (MAR) that an emergency has been declared

- Manning the Management Audio Call-in (MAC) providing informational announcement for serious emergencies per the direction of the ISEC or CIO. Notifies clients when services are restored.
- Updating the ISEC hourly or as events warrant

Resource Coordinator(s) (RC)

These are on-the-ground management resource responsible for the individuals that have made up the TAR. This role is typically in place when the emergency is at a College or location not directly staffed by UCit personnel.

- Monitors and facilitates the needs of TAR members
- Requests for assistance from outside resources or members of other internal organizations.
- Obtain technical expertise based on the emergency declared (in cooperation with the ISED and ISEC)
- <<Should not bug for status>>

Technical Alert Roster (TAR)

This is a listing of the level 3 technical resources that may be called upon in a declared emergency to provide the expertise required to resolve the issue.

- These personnel must be reliable and experienced in their field
- During a declared emergency, they are relieved of normal duty and report to the ISEC
- They may be required to relocate their base of operations to a field headquarters if required by the given emergency.

Management Alert Roster (MAR)

This is a listing of the management personnel that are to be alerted in a given declared emergency.

- This list may have members that are always alerted and members that are alerted only in a given circumstance.
- Members of this list may call the Management Audio Call-in (MAC) for updates

Scribe

This role documents ISERT activities and provides the collected documentation to the post mortem team

- Create a case file for the emergency
- Ensure information is properly collected and documented in near real time
- Follow the work plan established by the ISEC.

UC Information Security - Security Response Manager

Prior to an emergency, the ISEC is responsible for planning for the following:

- Establishing the “war room” during a computer emergency
- Providing appropriate networks, computers, phones, and faxes
- Establishing plans for the provision of food and lodging
- Maintains the Senior Management contact roster, soliciting updates semi-annually.
- Ensures that each UCit Department Director has an employee contact list..
- Maintains the Technical Alert Roster (TAR), soliciting updates semi-annually.
- Maintains the Management Alert Roster (MAR), soliciting updates semi-annually.

- Establish, maintain and publish a Technical Audio Conference number
- Establish, maintain and publish a Management Audio Conference number
- Establish, maintain and publish procedure that will direct helpdesk and other organizations to alert the ISEC of situations that may require review and possible request for declaration of emergency.

ISERT Post Mortem Team

The Post Mortem Team is assembled by the ISED, chaired by the CIO or the DCIO. This team is part of the Reactive Services “Maintenance”. Their responsibilities are:

- Sending final emergency reports to parties with a need-to-know
- Discussing procedural changes and updates
- Discussing configuration issues
- Deciding to conduct an investigation to determine the root cause and root effects of the emergency, discussing any task that was not completed
- Deciding whether it is necessary to determining the Total Cost of Emergency (TCI)
- Recommending updates to policies, procedures, standards and the Information Security Emergency Response Plan as necessary

UCit Help Desk

- Receives client notification of unavailable service. Checks client observations against ISEC list.
- Initiates communications for information security emergencies to the ISEC.

Network Operations Centers (NOC)

- Monitors Intrusion Detection and/or Intrusion Prevention Systems
- Monitors the Network
- Initiates communications to the ISEC as problems are detected or reported
- Provides technical resources via the TAR
- Provides assistance to the ISERT related to telecommunications
- Establishes new lines and communications bridges as directed by the ISEC
- Provides necessary communication lines for the ISERT War Room
- Assesses an emergency's impact to Wide Area Network and/or Local Area Network.
- Assists in identifying the impact to the perimeter and Internet facing environments.
- Assesses an emergency's routing and transmission impact
- Collects, stores, and assists in system audit data analysis as necessary for the routers and firewall.
- Provides log data to the ISERT as required
- Provides rule sets to the ISERT as required
- Provides assistance investigating PBX accounts and permissions
- Coordinates, implements, maintains and certifies all routing changes and OS changes to network devices.
- Implements changes to the firewall rule sets to assist in emergency containment as necessary

- Liaison as required with the telecommunications supply chain: OARnet, Cincinnati Bell, 3Com, Cisco, Aastra Intecom, Quest, Time Warner Communications, IBM, HP, Apparnet, Audible Magic, NetZentry, NetQOS, Silco, Peck Hannaford & Briggs and Simplex-Grinnell, Dell, Adtran, Static Power, APC, and Concorde

Server Operations

- Initiates communications to the ISEC as problems are detected or reported
- Provides technical resources via the TAR
- Monitors system log data
- Provides assistance in investigation of system account activity(s)
- Coordinates changes to the systems

Educational Technologies

- Initiates communications to the ISEC as problems are detected or reported
- Provides technical resources via the TAR

Information Security Emergency Response Steering Committee

- Appoint the Information Security Emergency Response Working Committee
- Receive requests for clarification and assistance from the Information Security Emergency Response Working Committee and advise them in their work
- Approve changes to the ISERP

Information Security Emergency Response Working Committee

- Meet at semi-annually to update the ISERP
- Receive recommendations from Post Mortem teams for improvements to ISERP
- Ongoing testing and evaluation of the ISERP operation

UC Public Safety

- Perform any law enforcement duties required
- Notify ISERT in the event of critical data loss during a disaster for which ISERT is not already involved
- Assist in interviews when requested
- Assist human resources during policy violations
- Coordinate with external law enforcement as required
- Liaison to Federal Bureau of Investigations (FBI) as requested by University Counsel
- Manage perimeter controls

Disaster Recovery Team

- Manages the development and maintenance of the Disaster Recovery Plan
- Receive declaration of disaster that would upgrade a information security emergency to a disaster
- Liaison with ISERT via command center
- Provide hourly DR status updates to the MAC
- Interfaces with the CIO and/or the ISEC to ensure proper integration and coordination between the ISERP and other crisis management plans, as required by event circumstances (Disaster Recovery Plan, Hurricane Preparedness Plan)

University General Counsel

- Provides guidance to the CIO regarding legal and regulatory aspects of the information emergency and its public disclosure
- Advises Human Resources regarding investigations involving employees
- Advises the CIO and/or ISEC regarding decision to simply protect its operations or to pursue civil or criminal actions
- Consults with the CIO and/or ISEC regarding involvement with law enforcement
- Advises the CIO and/or ISEC regarding involvement with regulatory agencies
- Reviews communications drafted by University Communications as required
- Liaison to external counsel

Human Resources

- Advises CIO and/or ISEC on personnel matters
- Participates in investigation interviews and furnishes legally permissible personal information as necessary
- Alerts the ISERT of any unusual employee behavior patterns during a information security emergency or investigation

University Communications

- Provides external communications in consultation with University Counsel
- Responds to all external media inquiries
- Liaison to external public relation firms
- Ensure internal communications are consistent with external communications
- Manages internal rumors and fields internal questions from the employee base that are not associated with an emergency
- Coordinates internal employee communications along with University Counsel, as necessary

IT Technical Support

- Coordinates change management and testing for the applicable UC server environment.
- Coordinates, implements, maintains and certifies the Operating System Environment for all UC operation systems.
- Assesses an emergency's impact to the server environment.
- Certifies and implements changes to the server environment.
- Coordinates and implements patches to the server environment
- Develops, maintains and implements hardening procedures for the server environment

E-Mail

- Responsible for the entire electronic mail system utilized by The University of Cincinnati.
- Coordinates changes to the electronic Mail environment
- Implements changes to messaging systems
- Assesses impact of email or messaging based malware (malicious code)
- Performs backup procedures on the server environment
- Liaison with IBM, Solaris, DNS-1, and SendMail
- Responsible for SAN administration

Database Administration

- Rebuild and implement installation for the databases
- Builds and configures the databases
- Provides backup and recovery services for the databases
- Overall security for the databases

Priorities in Emergency Handling

It is important to prioritize the ISERT actions to be taken during an emergency before an actual emergency occurs. Sometimes an emergency may be so complex that it is impossible to respond to everything at once; priorities are essential. Human life and national security will take first precedence and it is generally more important to save data than to save system hardware and software.

PRIORITY	TASK
1	Protect human life and people's safety.
2	Protect sensitive information from disclosure, abuse or misuse.
3	Protect regulated information to ensure no criminal, civil and/or administrative action occurred.
4	Protect critical information, systems, and networks from compromise, damage, alteration or corruption.
5	Minimize business disruption.
6	Certify that the integrity and availability of the areas affected have been restored to a Production Ready and Active Environment.

ISERT Example Emergency

Determining that an Emergency is Critical: Emergency Severity Levels

Information Security Emergency Defined

An emergency is any adverse event that threatens the confidentiality, integrity, or availability of university information assets, information systems, and the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or standard computer security practices is an emergency.

Adverse events may include, denial-of-service attacks, loss of accountability, or damage to any part of the system. Examples include the insertion of malicious code (e.g. viruses, Trojan horses, or backdoors), unauthorized scans or probes, successful and unsuccessful intrusions, and insider attacks. See Vangelos.

Emergencies as defined above vary in their impact on the University and in the degree of threat they pose; consequently not all emergencies require the same response. Emergencies with high impact and high threat involve high risk and great vulnerability to the University; such high risk emergencies are called 'information security emergencies' and require that a Information Security Emergency Response Team (ISERT) be assembled to apply appropriate response. Non-information security emergencies are emergencies with either low or acceptable risk. A non-information security emergency could become critical if its visibility could impact the reputation of the university.

Non-information security emergencies also have appropriate response; however procedures for non-information security emergencies are not outlined in this policy.

An emergency is declared to be critical and a ISERT assembled in one of the following ways:

- A member of the Emergency Response Steering Team declares it to be critical.
- Information Security Emergency Coordinator declares it to be critical.
- An appropriate University official declares to be critical.
- NOC staff declare it to be critical because the emergency is on the following list of examples information security emergencies approved by the Emergency Response Steering Team.

Examples of a Information Security Emergency

The following examples of 'information security emergencies' are given here to provide guidance to the ISEC in determining if an emergency is critical:

1. Real time registration failure. The first time that real time registration was used on the Oxford campus, scarcity of courses resulted in overpowering the web servers and the database. Registration times for each group had already been advertised so could not be changed easily. There was no protocol in place for students to look for alternate times. It took 2 days to fix the problem. October 2001. Impacted availability.
2. Slammer. April 2003. Blaster worm. August 2003. Impacted availability.
3. EPO server accessed by unauthorized user. E-Policy Orchestrator pushes virus protection and other security policy. After an intruder logged into the server it was necessary to show that no client vulnerability resulted from the hack. January 2005. Confidentiality, integrity, availability were all potentially compromised.

4. Murstein Fire. A fire in Murstein severed Network connections and threatened university information. The network was disconnected for over 24 hours. A whole department was without internet and computing service. April 2003. Availability was compromised.
5. President's e-mail signature forged. Someone sent an e-mail to all students declaring that classes were cancelled and forged the President's signature. 2003/03. This e-mail disrupted university business and was declared critical by the administration. Visibility.
6. E-mail forgery and Trojan horse on Good Friday. Someone sent an e-mail containing a Trojan Horse (Back Orifice?) forging the support desk signature and requesting recipients to execute it. 1999/04. Confidentiality, integrity, availability were all potentially compromised. Visibility.
7. E-mail migration. During migration of the e-mail system e-mail became unresponsive for 24-hours. Vendor interface with LDAP was a partial cause. October 2001. Availability was compromised.
8. A number of DoS attacks occurred one after the other; these collectively that impaired network service for extended periods of time for large portions of the campus. April 2004. Availability was compromised.
9. Network performances issues that impacted large sections of the campus persisted intermittently for weeks and were ultimately diagnosed as one major problem and several minor problems. October 2003. Review of this issue revealed that had the resources of a information security emergency been applied early on, it would have been solved quickly. Availability was compromised.
10. Electricians accidentally shorted a wire in a control panel that simulated pressing the red power down button. Hoyt Machine Room powered down. Full service took over 4 hours (12 hours) to restore. June 2003. Availability was compromised.
11. Butler County Fiber was severed by construction on a bridge in Hamilton. Telephone service to some university buildings was impacted for over 8 hours. April 2004. Availability was compromised.
12. Graphics Feed of Objectionable material to the dorms. 1998. This issue had the potential to publicly embarrass the university. It was important to avoid repetition. Visibility.
13. Road Runner clients in Southwest Ohio could not get to Miami. Road Runner had changed their router. It took 18 hours to resolve. Availability was compromised for a significant group of clients.
14. Acctgen clients notified of cancellation. There were 2000 people notified via e-mail that they are no longer in class and their account will be disabled in 30 days. There was no actual risk, but high visibility. Because students were notified that they are no longer in class, it was necessary to notify the Provost. Visibility.
15. WMUB lost internet service and therefore the only means by which to obtain weather and traffic information from Dayton. Subsequently they informed listeners that their internet service was down. This happened on three separate occasions. Equipment was purchased to avert risk of future occurrence. Although only one client (WMUB) was impacted directly, their many clients were impacted indirectly. This was also an embarrassment to the university. Availability was impaired.

The following kinds of emergencies are considered Critical

1. Destruction or unauthorized modification of data on university systems. The amount of data or the nature of the data will determine whether it is critical or not. Confidentiality, integrity, availability.
2. Unauthorized disclosure of student, staff or faculty data. Ohio law will determine whether this is critical or not. Availability.
3. A successful network intrusion that risks confidentiality, integrity, or availability on a wide scale. Availability.
4. A successful denial of service (DOS) attack against a significant portion of the university. Availability.
5. Widespread electronic mail system failure or slow down. Availability.
6. Critical application failures (i.e., SAP, UCFlex) that deny availability for more than 4 hours.

Examples

#	Example	Confidentiality	Integrity	Availability	Visibility
1.	Real time registration failure			yes	
2.	Slammer			yes	
3.	Unixgen accessed by unauthorized user	yes	yes	yes	
4.	Formscape server accessed by unauthorized user		yes	yes	yes
		yes			
5.	EPO server accessed by unauthorized user	yes	yes	yes	
6.	Murstein fire severing network service			yes	
7.	President's e-mail signature forged				yes
8.	E-mail forgery and Trojan horse on Good Friday		yes	yes	yes
		yes			
9.	E-mail migration slow down			yes	
10.	Widespread and lengthy DOS attacks			yes	
11.	Network performance impaired for weeks			yes	
12.	Hoyt machine room power down			yes	
13.	Butler county fiber severed at Hamilton bridge				yes
14.	Graphics feed of objectionable material				yes
15.	Road Runner clients from SW Ohio denied at MU				yes
16.	Acctgen clients notified of cancellation				yes
17.	Internet service to WMUB lost			yes	
18.	Destruction or unauthorized data modification		yes	yes	yes
19.	Unauthorized disclosure of data			yes	
20.	Wide scale network intrusions			yes	
21.	Widespread DOS (4 hours)			yes	
22.	Widespread e-mail system failure or slowdown				yes
23.	Failure of critical applications (4 hours)			yes	

Information Security Emergencies and Procedures

One way to decide whether an emergency should be treated as critical is to ask whether you wish the procedures in this document to be followed. If the emergency has small enough consequences it may not be worth assembling a team, following the procedures including filing reports to upper management. However, even a small event with big consequences should follow the procedures, possibly with a small team.

Emergency Severity Levels

As part of the initial emergency response process, the ISEC will need to make an assessment of the emergency's impact and assign an appropriate severity level. This severity level will be based upon the potential impact to the operations or reputation of The University of Cincinnati, and/or their students, faculty, and/or staff. An emergency's severity level dictates the initial response and management activities associated with the event. As emergency management activities continue, further assessment may effect a reassignment to a lower severity level. In this phase of the Emergency Response Plan for The University of Cincinnati, only emergencies whose severity level is 'critical' are managed; however, other severity levels are outlined below for completeness.

Critical Level

Successful penetration or denial-of-service attack(s) detected with significant impact on operations: very successful, difficult to control or counteract, large number of systems compromised, significant loss of confidential data, loss of mission-critical systems or applications, admin/root compromise, user account compromise, illegal file server share access. Significant risk of negative financial or public relations impact.

Medium Level

Penetration or denial-of-service attack(s) detected with limited impact on operations. Minimally successful, easy to control or counteract, small number of systems compromised, little or no loss of confidential data, no loss of mission-critical systems or applications. Widespread instances of a new computer virus or worm that cannot be handled by deployed anti-virus software that may require corporate-wide activations of ISERT and/or site-administrators. Illegal mirrors and unapproved content. Small risk of negative financial or public relations impact.

Low Level

Significant level of network probes, scans and similar activities detected indicating a pattern of concentrated reconnaissance. Intelligence received concerning threats to which systems may be vulnerable. Penetration or DoS attacks attempted with no impact on operations. Isolated instances of a new computer virus or worm that cannot be handled by deployed anti-virus software.

Information Security Emergency – Any unexpected or unauthorized change, disclosure or interruption to The University of Cincinnati's information resources that could be damaging to our students, staff, faculty, and/or reputation.

Team Makeup by Position Title

Chief Information Officer:

ISED:

Emergency Response Coordinators:

Group 1 – Days of the month 1 -10: List 6 names here

A thru C

Group 2 – Days of the month 11-20: List of 6 names here

D thru H

Group 3 – Days of the month 21-end: List of 6 names here

I - Z

Forensic Resources: List of 8 names here

Information Security Emergency Team Members

Information Security Emergency Team Members:

Any coordinator could be asked to serve on the team. Any forensic resource could be asked to serve on the team

List of 8 additional tech staff here

You may draft any UCit staff that you need. The above staff are trained and area therefore first choice

Appendix A – Information Security Emergency Review Report

NOC Emergency Number (NOC Remedy Ticket Number) _____

Date of Emergency _____

Name of CIR Coordinator _____

For all information security emergencies the information security emergency coordinator (SEC) must fill out this form within one week of the resolution and file the report with the office of the Vice President of Information Technology. Any relevant documents should be attached.

Preparation

- Were controls applicable to the specific emergency working properly? y/n
- What conditions allowed the emergency to occur?
- Could more education of users or administrators have prevented the emergency? y/n
- Were all of the people necessary to respond to the emergency familiar with the emergency response plan? y/n
- Were any actions that required management approval clear to participants throughout the emergency? y/n

Detection

- How soon after the emergency started did the organization detect it?
- Could different or better logging have enabled the organization to detect the emergency sooner? y/n
- Does the organization even know exactly when the emergency started? y/n
- How smooth was the process of invoking the emergency response plan? 1 2 3 4 5 (5 = very smooth)
- Were appropriate individuals outside of the emergency response team notified? y/n
- How well did the organization follow the plan? 1 2 3 4 5 (5 = very well)
- Were the appropriate people available when the response team was called? y/n
- Should there have been communication to inside and outside parties at this time; y/n
- and if so, was it done? y/n
- Did all communication flow from the appropriate source? 1 2 3 4 5 (5 = all did)

Containment

- How well was the emergency contained? 1 2 3 4 5 (5 = very well)
- Did the available staff have sufficient skills to do an effective job of containment? 1 2 3 4 5 (5 = all did)
- If there were decisions on whether to disrupt service to internal or external customers, were they made by the appropriate people? y/n
- Could changes to the environment make containment easier or faster in the future? y/n
- Did technical staff document all of their activities? 1 2 3 4 5 (5 = all)

Eradication and Recovery

- Was the recovery complete (no data permanently lost)? y/n
- If the recovery involved multiple servers, users, networks, etc., how were decisions made on the relative priorities?
- Did the decision process in the previous question follow the emergency response plan? y/n
- Were the technical processes used during these phases smooth? y/n
- Was staff available with the necessary background and skills? y/n

Appendix B – Who Contacts Whom

Who	Contacts Whom
CIO	<ul style="list-style-type: none"> • President / PEC • HR • University Counsel • University Communications • Safety and Security • Press
DCIO	<ul style="list-style-type: none"> • CIO when the DCIO is working with an emergency
SEC	<ul style="list-style-type: none"> • CIO (or the DCIO if the CIO is not available) • Safety and Security • ASEC
ASEC	<ul style="list-style-type: none"> • SEC (or the CIO if a CID is not available) • NOC • CIR Team Members (NOC can assist) • UCit Management (listserv) • Primary Technical and Management Alert Roster Manager and Members (TCM, TAR, MCM, MAR) • RCs and Secondary TARs
University Communications	<ul style="list-style-type: none"> • Press
TCM	<ul style="list-style-type: none"> • ASEC • P-TAR • S-TARs
MCM	<ul style="list-style-type: none"> • ASEC • RCs
TAR Members	<ul style="list-style-type: none"> • TCM
Resource Coordinator	<ul style="list-style-type: none"> • MCM • Associated S-TAR
Constituency – Faculty Staff and Student	<ul style="list-style-type: none"> • MCM
Constituency – Technical	<ul style="list-style-type: none"> • TCM

Appendix C – Time Guidelines

Notify ISEC if emergency is suspected to be critical	10 minutes
Notify NOC if emergency declared critical	Immediate
Notify CIO if emergency declared critical	Immediate
Length of outage before time makes it critical	
Whether to do forensic investigation	10 minutes to get answer
Length of time between updates to the CIO	1 hour or as requested
Conduct Post Mortem evaluation	2 weeks

Appendix D – Tabular Summary of Data Valuation

Not Classified

All information not otherwise identified

Unrestricted

Information available to employees for normal operational use or to the public based on appropriate request for disclosure of information

- General financial data
- Student directory information (non opt-out)
- Unique ID
- Non-confidential personnel data

Internal

Information that the organization and its employees have a legal, regulatory, or social obligation to protect. Intended for use solely within defined groups in the organization

- Employee ID
- Student ID
- Employee benefit information
- Student non-directory information

Sensitive or Confidential

Information intended solely for restricted use within the organization and is limited to those with an explicit, predetermined “need to know”. Disclosure could result in severe personal or financial damage to individuals or the organization

- SSN
- Passwords/PINS
- Credit card numbers
- Digitized signatures
- Encryption keys
- Medical Records – Employee, student, research

Appendix E – Tactical Organization Equipment list

To be completed in cooperation with UCit DR and Public Safety DR representatives.

Appendix F – Components of a Notification Letter

Edit the following components into a letter of notification or web site statement. Headings are boldface, several examples follow most headings. Edit the sample text into your letter and delete the heading. Don't disclose anything that hampers the investigation or gives additional information to those who would do harm.

What happened?

(E.g. A server/laptop/desktop was breached/stolen/lost in <school or location>)

In December 2004, campus officials were notified of the theft of an [department name] laptop computer

When did the breach occur and/or when was it detected?

How was it detected?

What data was potentially compromised?

This computer contained a list of [department] student employees. The list included the names and Social Security Numbers of the students.

How much data was compromised?

For whom was data compromised?

Why you are being notified.

We are notifying you of this security breach because you are one of the students whose personal information was present on the laptop. Although we have no evidence that an unauthorized individual has actually retrieved and is using your personal data, we are bringing this emergency to your attention, in accordance with California law, so that you can be extra alert to signs of any possible misuse of your personal identity.

What steps are/were being taken?

(e.g. machine taken off the net, law enforcement (local/FBI), Credit card companies notified (for cases where contact information is needed about cardholders), etc)

Is any data known to be fraudulently used or is notification precautionary?

What steps should individuals take?

(e.g. place a fraud alert with the credit bureaus, contact credit card companies, close accounts, etc.)

Although there is no evidence that an unauthorized person has obtained your personal information and is using it, there are some steps you can take, exercising abundant caution, to protect yourself. First, you may place a fraud alert with credit bureaus and/or periodically run a credit report to ensure accounts have not been activated without your knowledge. If you determine that an account has been fraudulently established using your identity, you should contact law enforcement and the financial agency. The following references provide additional information about identity theft:

- Federal Trade Commission website on identify theft (<http://www.consumer.gov/idtheft/>)
- Social Security Administration fraud line at 1-800-269-0271
- Major Credit Bureau Numbers
 - Equifax 1-800-525-6285
 - Experian 1-888-397-3742
 - Trans Union 1-800-680-7289
- Identify Theft Victim Checklist (<http://www.privacy.ca.gov/sheets/cis3english.htm>)

Apology or statement of commitment to security

We regret that your information may have been subject to unauthorized access and have taken remedial measures to ensure that this situation is not repeated. The University of Cincinnati is committed to maintaining the privacy of student information and takes many precautions for the security of personal information. In response to emergencies of theft like this one and the increasing number of internet-enabled computer attacks, the University is continually modifying its systems and practices to enhance the security of sensitive information. We sincerely regret any inconvenience this emergency presents to you.

Anticipated next steps, if any.

e.g. intention to notify if any additional information becomes available?

Who to contact for additional information

Contact/name, number, hours of availability, web site, hotline, email address, etc.

Should you have further questions about this matter, please contact [name of contact], [title of contact], at [email address of contact] or [phone number].

Signature

Who makes most sense – president, dean, other contact familiar to the individual, consider multiple signatories for different constituent groups.

Appendix F – Forensic Evidence Methodology

Once an emergency has been declared and a decision has been made to preserve electronic evidence for use in either administrative, civil or criminal remedies, specific steps should be taken to ensure integrity of data and preservation of evidence.

The ISERT charter, as defined in Section 1 of the ISERP, is to provide business, service and data preservation and is not chartered with maintaining computer forensic capabilities. Therefore, this methodology is not intended to be in-depth, but rather intended to highlight the importance of evidence handling procedures before outside computer forensics teams are called upon.

The below list is by no means all-inclusive and should not limit the scope of evaluation as to where digital evidence may only be found.

TYPE OF EMERGENCY	POSSIBLE LOCATIONS OF RELEVANT EVIDENCE
Network Intrusion	System Logs User Logs Proxy Logs Router & Firewall Logs
Email Threats	Mail Servers Router & Firewall Logs Individual Workstations Backup Tapes
Internal Employee or Contractor Activity	System Logs Mail Server Logs User Logs Proxy Logs Router & Firewall Logs Individual Workstations Electronic Organizers Removable Media

Definitions:

Electronic Evidence

Electronic Evidence is information and data of suspected investigative value that is stored on or transmitted by an electronic device. As such, electronic evidence is latent evidence in the same sense that fingerprints or DNA evidence is latent. In its natural state, data contained in the physical object that holds electronic evidence such as a server, desktop PC or hand held device such as PDA's like a Palm Pilot, iPAQ or Handspring Visor cannot be seen. Equipment and software are required to make the evidence visible.

Electronic evidence can be found in user created files, encrypted files, and computer created files or in hardware components such as Network Interface Cards (NIC), routers and switches as well as on removable media such as floppy and zip disks, CD and DVD discs, USB thumb drives and tape. Other hardware devices such as all-in-one copiers, scanners, printers and fax machines often maintain user access records and temporary buffer files, which may contain valuable data. Electronic evidence can be altered, damaged, or destroyed by improper handling or examination. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion. When dealing with electronic evidence, general forensic and procedural principles should be

applied. The Federal Guidelines for Searching and Seizing Computers is an excellent resource for an in depth information on this topic.

Chain-of Custody

Chain of Custody pertains to the documentation and securing of evidence items recovered during an emergency. Each item is assigned a unique identifying number or name, initialed by the team member recovering the item and documented in a format listing each item, where it was located, the date and time of recovery, and the team member involved. Items are then secured in a controlled environment under limited access. A record is kept documenting each person who comes into contact with the evidence item and the purpose for that persons possession of the item. Accountability for ensuring this process is adhered to lies with the SEC, with responsibility for following this procedure residing with each team member encountering items of an evidentiary nature.

In general, the following concepts should be applied:

- Actions taken to secure and collect electronic evidence should not change the evidence.
- Persons conducting examination of electronic evidence should be trained and preferably certified for this purpose.
- Activity relating to the seizure, examination, storage, or transfer of electronic evidence should be fully documented, preserved, and available for review.

Many emergency investigations, especially those expected to result in criminal or civil legal action will include a forensic analysis component. The ISERT members will frequently serve dual roles as investigators and forensic analysts. Each role has distinct areas of responsibility.

Note: Emergency responders should use caution when seizing electronic evidence devices. The improper access of data stored in electronic devices may violate provisions of Federal Law such as the Electronic Communications Privacy Act (ECPA). Additional legal process or policy may be necessary.

Collecting Evidence

Securing and Evaluating the Scene

After securing the scene or equipment, the first responder should visually identify both conventional and electronic evidence and determine if perishable evidence exists. The first responder should evaluate the scene and formulate a search plan. Do not at this time alter the condition of any electronic devices unless a threat to the safety of persons is indicated or business operations are such that continued operation or non-operation threatened the continued function of vital business operations. This decision should be made by the CIO, ISEC or their designee.

If a device is off, leave it off. If it is on, leave it on and seek additional assistance

Protect perishable data both physically and electronically. Perishable data can be found on pagers, caller ID boxes, electronic organizers, cell phones and other similar devices. The first responder should keep in mind that any device containing perishable data should be immediately secured, documented and if possible photographed.

- Observe and document the condition and location of the computer system including power status of the computer (on, off, or in sleep mode)
- Identify and document related electronic components that will not be collected.
- Photograph, if possible, the entire scene to create a visual record as noted by the first responder.

- Photograph and document the front of the computer or location of a device and take written notes on what appears on the monitor screen. Active programs may require videotaping or more extensive documentation of monitor screen activity.

Handling Evidence

The ISEC is accountable for ensuring chain-of-custody on all evidence collected. Individual ISERP team members are responsible for protecting the integrity of any evidence they work with. Whenever possible, analysis should be performed on copies of the evidence not the originals. Evidence will be handled in accordance with the guidelines set forth within this plan. An effort will be made to conduct analysis of digital evidence only on copies of the suspect media. A forensic duplicate of the original evidence will be made as soon as possible, and will be handled as much as possible in the following manner:

1. A hash (checksum, message digest) of the suspect media will be made.
2. Forensic duplicate of the media will be made. The forensic image(s) may be on tape, disk, magneto-optical cartridge, CD-R, DVD+R or any combination thereof as determined by the investigator.
3. A hash of the forensic duplicate will be made.
4. The hashes of the original and forensic duplicate will be compared to verify accuracy.
5. If necessary, the forensic image may be remounted to recreate its original configuration.
6. Suspect files or data may be transferred to CD/DVD or other media to aid in their review. In such circumstances, it should be noted that the media contains only select files and is not a forensic image of the original media.

NOTE: Many electronic devices contain sensitive memory that requires continuous power to maintain the data such as a battery or AC power. Unplugging the power source or allowing the battery to discharge can cause a loss of data. After determining the method of collection, collect and store the power supply adaptor or cable if present with the recovered device.

Analyzing Evidence

Forensic analysis is a technical examination rather than investigative in nature, even though the analysis is part of an emergency investigation. When conducting an analysis, the analyst must adhere to the following:

1. Analysis must be an unbiased examination of the evidence submitted. The analyst's focus must not be on connecting the evidence to the crime, but rather on analyzing the media in accordance with the investigator's request. Both positive and negative evidence must be documented. Analysts must go beyond the initial indicators of criminal involvement to insure no other possibilities exist. This insures that the investigator has the best possible information from which to work, and that the analyst appears to the court as an impartial examiner.
2. Forensic analysis does not pronounce or imply guilt. The purpose of forensics analysis is to determine whether indicators exist which can tie the suspect hardware to the emergency under investigation. Files and/or data obtained from the media may indicate that the suspect computer, hard drive, or whatever may have performed a certain task, but not that a specific person sat at the keyboard and committed some heinous act.
3. Report only verifiable information. Even if the analyst knows who owns the suspect equipment, it is a quantum leap to say that person was using it at the time of the crime.

4. Let the investigator tie media analysis findings to the investigation. Analysis may indicate or verify that the suspect computer connected to a certain IP address (for example). This doesn't necessarily mean it was connected to a specific person's computer.
5. Unless critical to the analysis, do not use names in the report. Instead, refer to "subject," "suspect," or "victim."
6. Identify the evidence being analyzed as thoroughly as possible. The analyst may have to identify the item again in a court of law. This is not the place to be unsure. Analysts should make their own unique mark on the evidence to aid in later identification.
7. Write the report for the uneducated, not another analyst. Explain uncommon terms – terms such as hash, clusters, tracks, sectors, etc. should all be explained the first time they are used. Explain processes – what/why is certain information recorded in a file.
8. Be precise. Statements such as "numerous," "many," "multiple hundreds," etc. should be avoided. Specifically state the finding, as well as the precise locations of information.

Reporting Findings

The complete evidence collection and subsequent analysis process should be memorialized and documented thoroughly. The format of this documentation report is as follows:

1. Summary of Analysis. A short, concise description (no more than about two pages) that summarizes the findings documented in the remainder of the report.
2. Actions Taken. A description of the circumstances that prompted the ISERP activation, actions taken, and personnel involved
3. Receipt of Evidence. Documentation of when, where, and from whom the evidence was received (or taken).
4. Physical Analysis. A visual evaluation of the evidence that was examined. Complete documentation of the items to include brand name, model number, and serial numbers.
5. Forensic Duplication. Document exactly how the image was made (for digital evidence). Include the software and hardware used to make the image, and the hash comparison results.
6. Analysis. Document every step taken in the analysis of the media. Explain what tools were used and what was or was not discovered as a result of these processes. Document such information as number and size of sectors, operating systems, significant software, anti-virus and crash-guard software, etc.
7. Evidence Disposition. Document how and when the evidence was returned or the manner in which it was disposed.

Appendix G – UCit Disaster Recovery Plan



Appendix H – Order of Succession for CIO Duties

<<>>

Appendix B

Gartner Research

Publication Date: 20 January 2006 ID Number: G0013736

Ten Recommendations to Prevent a Successful Attack

Amrit T. Williams

It is an unachievable goal for most organizations to prevent all bad things from occurring. The goal of a security program should be to limit the probability of a successful attack and, if an incident does occur, limit its impact on the organization.

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.

WHAT YOU NEED TO KNOW

Organizations cannot prevent all attacks from occurring. However, they can follow these 10 recommendations to limit the probability of a successful attack.

STRATEGIC PLANNING ASSUMPTION(S)

Organizations that implement pre-incident security processes and controls, in addition to reactive processes and controls, will experience an 80 percent decrease in successful attacks (0.8 probability).

ANALYSIS

Most organizations focus most of their security resources on reactive security technologies that offer value at the time of an incident or after it occurs (post-incident). This is certainly an important aspect of a security program; however, organizations must recognize that maturing their IT security management program requires implementation of pre-incident technology controls and processes.

The internal network and the external threat environment are very dynamic, and what seemed secure yesterday may become the biggest hole in your network tomorrow. Unfortunately, many organizations believe that once they deploy a security technology, the job of securing the network has been completed. Security technologies require continuous updates to ensure they are able to react to the latest threats, as is primarily the case with signature-based tools, and to ensure proper configuration based on the threat environment, as is the case with intrusion prevention system (IPS) blocking.

The most-effective method for securing the network and limiting the probability of a successful attack requires an understanding of the external threat environment and the internal organizational security posture, and using that information to drive the deployment and configuration of network and desktop security technologies. This understanding must be coupled with the definition, audit and enforcement of corporate security policies.

What follows are the top 10 recommendations to limit the probability of a successful attack.

1. Perform vulnerability assessment scanning at least once a week and immediately following any technology changes, and act on the data.

Vulnerability assessment data will provide extensive information on the state of devices on the network, including open ports, services, applications, protocols, operating systems and vulnerabilities. The three main methods of obtaining this in-depth data are host-based agents, active network scanning and passive network monitoring. Gartner recommends organizations deploy at least two of these three methods. Network-based assessment technologies generally provide the foundation for vulnerability assessment scanning. They should be used by the security group to remotely audit the IT environment without the requirement of an agent or passing administrative user name and password credentials to the scanning tool.

Vulnerability assessment scanning provides three key capabilities:

Information on the state of endpoints within the IT environment to understand an organization's internal security posture — Coupled with a security information and event management system (SIEM) product or other vulnerability reporting tool, this can provide comparison of vulnerabilities

Data used for the purpose of modifying the devices to eliminate the root cause of vulnerabilities and exposures, as well as to identify policy violations

Intelligence to implement and configure shielding controls to protect the environment prior to removing the root cause — This endpoint intelligence is critical to determining the best course of action to defend against an ever-changing threat environment.

2. Include network vulnerability assessment scanning tools as part of the overall network access control (NAC) audit process.

NAC is one of the best ways to deal with unmanaged nodes accessing the network, to limit the spread of an infection from one of the devices, and to limit network disruption. Most NAC implementations include scanning the endpoints through the use of static or dynamic agents; however, this does not provide 100 percent coverage of all nodes or any ability to probe all unmanaged nodes, especially those that are not capable of accepting an agent. To ensure the ability to audit unmanaged nodes against the NAC policy, organizations should include network-based vulnerability assessment scanning tools that can remotely identify the state of the unmanaged node without the use of agents or credential passing.

3. Use a third-party provider to perform a thorough penetration test annually and following any major modifications to the IT environment.

Penetration testing aims to provide a thorough assessment of an organization's security defenses and is performed by individuals using a set of tools and processes to actively identify security posture, weaknesses, vulnerabilities and exposures. Different from a vulnerability assessment, which attempts to identify the state of endpoints against a database of known vulnerabilities, penetration tests attempt to identify all potential exposures throughout the IT environment or system.

Penetration tests are an excellent method to highlight design weaknesses, technical defects and vulnerabilities. Their output is well-suited for driving networkwide security enhancements. In the case of service-oriented architecture, application service providers (ASPs), embedded systems or other scenarios in which an organization has limited visibility and control, a penetration test can help provide much-needed visibility.

Penetration tests should be performed by a qualified service provider. These services are offered by large companies (such as Ernst & Young, PricewaterhouseCoopers, Deloitte & Touche, and IBM) as well as security service providers (such as Symantec and Internet Security Systems). When an organization does not have the ability to perform a penetration test against systems out of their control, they should require the upstream provider or ASP to perform these tests and provide a report on their output.

4. Use external threat intelligence to get perspective on the changing external threat environment, and update defenses as soon as exploit code is identified.

The external threat environment is continuously changing, and it is a difficult task to manually track the latest threats in a timely manner. Threat intelligence services can provide up-to-date and organizationally relevant threat information to assist in prioritizing security decisions, whether they be deploying patches and updates, reconfiguring firewalls and e-mail servers, or implementing specific blocking capabilities in IPS products.

These services can be provided directly to an organization, either through a threat intelligence service, or as part of a bundle with a security product. If either of these are not available to the

5. Expand vulnerability management activities to include networking devices, commercial enterprise applications and database applications, as well as internally

developed Web applications.

Most organizations focus their vulnerability management activities on Microsoft desktops, scanning these devices for critical vulnerabilities and then applying patches as the threat reaches a certain level of risk. Unfortunately, the vulnerability landscape is changing. Over the past several years, there has been a dramatic increase in published critical vulnerabilities against networking devices (such as Cisco), commercial enterprise and database applications (such as Oracle), and internally developed Web applications.

Commercial vulnerability assessment tools can remotely scan many of these devices and applications to identify their configuration, as well as if they have any publicly known vulnerabilities or exposures. This information, even if it simply identifies base-level information, can assist in driving the deployment and configuration of other security technologies responsible for providing security controls for these devices and applications.

In the case of Web applications, Web application scanners will assess the state of the Web application to determine poor coding or configuration practices that can lead to an attack. Generally these tools do not scan the Web applications against a database of known vulnerabilities, but instead they look for signs that are indicative of vulnerabilities. Cross-site scripting, command injection and weak authentication parameters are all examples of the types of weaknesses these tools aim to identify.

6. Expand the vulnerability management process to shield the environment in the face of critical threats, as opposed to rapid patching.

Many organizations, faced with critical vulnerabilities and threats, attempt to patch their systems as quickly as possible. Although eliminating the root cause is important, it should not be the first step once a critical vulnerability is identified. The first response to a critical threat should be to shield the environment using deployed security defenses. In-line IPS, desktop security product configurations, and other security and networking devices can all be used to prevent a successful attack while the organization takes the proper time to test the patch for application compatibility and to ensure no system disruption.

7. Frequently update security defenses with the latest signatures, updates and configuration changes.

Organizations spend a significant amount of money and resources on deploying security technologies on the desktop and throughout the network. Their effectiveness in preventing an attack is dependent on these tools' running the latest updates to address an ever-changing threat environment. Deploying security technologies is only one part of implementing adequate security controls. These controls must be kept up to date. Security technologies should be updated with the latest signature and configuration files weekly or bimonthly, as well as immediately following a critical change in the external threat environment. Ideally these tools should be configured to check for updates every 24 hours.

8. Continually review and update the desired configuration state of devices on the network based on internal security posture, external threat environment and corporate policy.

A strong security program includes defining, auditing and enforcing policy. Security configuration management tools are used, as part of a vulnerability management program, to perform these tasks against managed endpoints in the environment. To be effective the policy, which includes

Publication Date: 20 January 2006/ID Number: G00137363 Page 4 of 6

The internal security posture (new vulnerabilities are identified)

The external threat environment (exploit code is actively exploiting vulnerabilities)

The corporate security policy (the gold image is modified to include new patches, software or configurations)

Review and update the security configuration management policies often, and ensure there is a mechanism for supporting the dynamic nature of the internal IT environment and the external threat environment.

9. Integrate identity and access management (IAM) with SIEM to identify any patterns of activity that may indicate suspicious behavior that can lead to an incident.

Integrate IAM data into the SIEM framework, and identify suspicious behavior by correlating user application access with established IAM policies. Most SIEM activities focus on the network view, looking for events associated with devices and paths through the network. Internal users pose a significant threat to an organization's security, and organizations must monitor user events not only to look for suspicious behavior, but increasingly to satisfy regulatory compliance requirements.

10. Use network behavior analysis (NBA) tools to detect suspicious behavior on the network that may indicate an impending attack.

NBA tools provide networkwide visibility that can identify suspicious behavior indicative of an impending or in-progress attack. These tools can also be used to provide networkwide vulnerability assessment information in the form of policy violations (for example, no FTP traffic on this network segment or no Microsoft servers should be running on this segment). This level of information requires a definition of policy, and then use of the tool to audit against the policy. Additionally this data should be integrated into the SIEM framework for correlation with other system events, providing a high-level overview of an impending or in-progress attack from multiple network and security control perspectives.

Recommended Reading

"Agile Processes Improve Enterprise Corporate Security Programs"

"Improve IT Security With Vulnerability Management"

"Establish Vulnerability Management Processes to Protect Networking Devices"

"Magic Quadrant for Security Information and Event Management, 2H05"

"Magic Quadrant for MSSPs, North America, 2H05"

Acronym Key

ASP	application service provider
IAM	identity and access management
IPS	intrusion prevention system
NAC	network access control
NBA	network behavior analysis

Publication Date: 20 January 2006/ID Number: G00137363 Page 5 of 6

SIEM	security information and event management system
-------------	--

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road Stamford, CT 06902-7700
U.S.A. +1 203 964 0096

European Headquarters

Tamesis The Glanty Egham Surrey, TW20 9AW UNITED KINGDOM +44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd. Level 9, 141 Walker Street North Sydney New South Wales 2060 AUSTRALIA +61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd. Aobadai Hills, 6F 7-7, Aobadai, 4-chome Meguro-ku, Tokyo 153-0042 JAPAN +81 3 3481 3670

Latin America Headquarters

Gartner do Brazil Av. das Nações Unidas, 12551 9º andar—World Trade Center 04578-903—São Paulo SP BRAZIL +55 11 3443 1509

Publication Date: 20 January 2006/ID Number: G00137363 Page 6 of 6