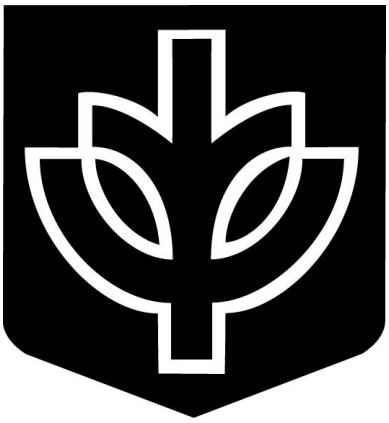
A FRAMEWORK FOR INCIDENT RESPONSE (DRAFT)



Information Security Team
DePaul University
1 East Jackson Boulevard
Chicago, Illinois 60604 US
https://infosec.depaul.edu/

13th December 2002

Copyright Notice

Contents

1 Summary

Computer and network security incidents increase exponentially as the Internet continues to grow and new technologies are developed and deployed. DePaul University relies on the Internet and such technologies for academic research and development, mission-critical business processes, communication, etc. This procedural framework attempts to define a concrete methodology for responding to computer and network security incidents.

2 Terminology

The terms ABNORMAL, ANALYSIS, EVENT, EVIDENCE, FORENSIC, INCIDENT AND NORMAL are listed here for reference to be used throughout this document. These terms are defined for us as found in [1].

- ABNORMAL: "Not conformed to rule or system; deviating from the type; anomalous; irregular."
- ANALYSIS: "to unloose, to dissolve, to resolve into its elements;"
- EVENT: "That which comes, arrives, or happens; that which falls out; any incident, good or bad."
- EVIDENCE: "That which makes evident or manifest; that which furnishes, or tends to furnish, proof; any mode of proof; the ground belief or judgement; as, the evidence of our senses; evidence of the truth or falsehood of a statement."
- FORENSIC: "Belonging to courts of judicature or to public discussion and debate; used in legal proceedings, or in public discussions; argumentative, rhetorical; as, forensic eloquence or disputes."
- INCIDENT: "Coming or happening accidentally; not in the usual course of things; not in connection with the main design; not according to expectation; casual; fortuitous."
- NORMAL: "According to an established norm, rule or principle; conformed to a type, standard, or regular form; performing the proper functions; not abnormal; regular; natural; analogical."

2.1 Requirements Terminology

The terms MUST, MUST NOT, SHOULD, SHOULD NOT AND MAY are defined per [2] and listed below.

- MAY: "This word, or the terms 'REQUIRED' or 'SHALL', mean that the definition is an absolute requirement of the specification."
- MUST NOT: "This phrase, or the phrase 'SHALL NOT', mean that the definition is an absolute prohibition of the specification.
- SHOULD: "This word, or the adjective 'RECOMMENDED', mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course."
- SHOULD NOT: "This phrase, or the phrase 'NOT RECOMMENDED' mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label."

- MAY: "This word, or the adjective 'OPTIONAL', mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).

3 Objectives

The primary objectives of the incident response and handling procedures are to:

1. RESTORE and MAINTAIN normal academic and business continuity.
2. INCREASE DEFENSE and SURVIVABILITY against future incident.
3. DETER future incident by acts of investigation and prosecution.
4. EDUCATE through acts of intelligence or counter-intelligence actions.

4 Severity Levels

Each incident should be assigned a severity level. This severity level may be modified by investigators, as required, throughout the duration of the investigation. A severity level should not be modified after the investigation cycle of an incident response period has completed.

4.1 Level One

A Level 1 incident severity level represents an incident that is the most critical level. One, or more, of the following parameters should be met when assigning a Level 1 severity level.

1. Unauthorized disclosure, modification, destruction or deletion of sensitive information or data.
2. Disruption of business continuity and critical business processes or communication.
3. Impacts public long-term perception of the organization, either in part or whole.
4. Identity theft of an individual or group.

The manager(s) or operator(s) of resources involved in a Level 1 incident should be explicitly instructed not to use the resources until the Incident Investigation Coordinator establishes contact and defines further instruction.

4.2 Level Two

Level 2 severity levels are identified to have non-intrusive impacts on current services and represent passive attacks or monitoring of critical communication, possibly in effort to gain information for future attacks. The following lists qualifications for assigining a Level 2 severity level.

1. Passive interception of critical plain-text communications.
2. Disruption of non-critical business processes.
3. Extended enumeration of resources or data in effort to gain further information for future attack.
4. Continued harassment of an individual, psychologically or otherwise, against an existing, legally valid, Court Order.
5. Unauthorized use.

If an incident includes unauthorized use, the manager(s) or operator(s) of resources involved will be explicitly instructed not to use the resources until the Incident Investigation Coordinator contacts them with further instruction.

4.3 Level Three

Level 3 is defined as an incident involving harassment, whether intentional or non-intentional, or threats of resources and individuals of a computer or network system.

4.4 Level Four

Level 4 incident severity levels are defined only as non-evident and unsubstantiated rumors of incident.

5 Response Handling Roles

Any incident reported to the Incident Reponse Team or Security Team shall warrant investigation. A full-time member of the Security Team will act as the Incident Investigator and Coordinator (IIC). Any member of the Incident Reponse Team may act as the Incident Liaison (IL). The IL shall be assigned by the IIC on the basis of area of impact of the incident.

5.1 Incident Investigation and Coordinator

The Incident Investigator and Coordinator (IIC) shall assign the severity level to the incident and perform all investigative duties and technical analyses. Evidence collected during investigation should be supervised by the IIC in the event that further investigation and prosecution requires expert witness testimony.

IIC duties warrant unrestricted access to resources directly effected by the incident. Such access shall be monitored by the IL and MUST be granted at the request of the IIC for the extent of the investigation.

The IIC, in conjunction with the IL, shall determine the requirements and necessities of disrupting further services as part of the recovery from incident. The IIC shall coordinate document evidence and lifecycle of the incident and store evidence for future access, if deemed necessary.

5.2 Incident Liaison

The IL shall act as coordinator and liaison to resources required by the IIC. These resources include the following.

- Hardware resources.
- Personnel.
- Emergency fund allocation.

The Incident Liaison MUST also act as secondary witness to all modifications of computer and network systems in the event that forensic analysis will be performed. The IL MUST verify, as per the guidelines set forth in this framework, that evidence has been collected without disruption or corruption, and in a timely manner. The IL should oversee documentation and reporting of all factual information, by all affected parties and the IIC, and verify that said documents are delivered, as necessary, to executive level personnel.

6 Allocation of Resources

The IL may call upon the allocation of emergency resources during mitigation or investigation of an incident. These resources are required to effectively ensure the primary objectives, as defined in the section entitled “Objectives” in this memo, are successfully met.

A Level 1 or Level 2 incident may require the intervention of law enforcement officials depending on the scope and severity of the incident. The Incident Response Team will recommend such actions to the Director of the involved division for Information Systems and business related incidents, the Dean of the school during academic related incidents, and possibly the Vice President of the department or Executive Vice President. During all dialogue with law enforcement officials the legal counsel will be included.

7 Procedures

Computer incident response is based on documented and untampered evidence. This evidence should be gathered through interviews, forensic analysis, and reports. Unsubstantiated rumors and comments should not be included in reports unless it is preceded as being deemed the "best guess" of the witness. The response handling stage and investigation should proceed in a methodical manner following the guidelines listed below.

7.1 Identify Affected Resources

The IIC and IL will act with system personnel to determine the area and scope an incident may cover. This step may be revisited throughout the investigation as more facts and evidence surface.

7.2 Incident Assessment

After determining the initial scope and coverage of the incident, an assessment MUST be performed by the IIC, in conjunction with the IL and system personnel, to determine the severity level. This initial assessment may also require the IIC to recommend further services be interrupted for proper investigation.

7.3 Assign Event Identity and Severity Level

All incidents require a unique identifier that should remain collission-free, allowing extensible tracking and archiving of incidents for historical reference. The incident identity is to be assigned by the IIC. Following name assignment, a severity level must be assigned to the incident. The severity level will determine the procedures and resources required to successfully respond to and recover from the incident, and MUST be chosen with care. If an incident falls between two severity levels, the more critical severity level should be chosen.

7.4 Assign Incident Task Force Members

The IIC, assisted by the IL, will coordinate a task force to resolve the incident. This task force may include technical managers of resources, division managers, etc. Level 1 incidents MUST require incident specific non-disclosure agreements to be signed, digitally or otherwise, by participants not actively involved in the Incident Response Team. This agreement MUST be distributed by the IL to any members participating in a task force during the initial stages of the response coordination.

7.5 Containing Threats

The initial assessment of the incident may require immediate containment. The IIC and IL are responsible for determining risks the incident poses and if the scope of the

incident will increase. Where necessary, threats should be contained by removing the suspect resources from normal operations.

7.6 Evidence Collection

Any information pertaining to an incident, regardless of the extent to which it may manifest itself, is evidence. This information will range from interviews with administrators, log files, unlinked files, exploit code left from an attacker, physical descriptions of the location and type of physical hardware, list of anomalous access times, bitstream copies of hard disks, kernel messages, processes running on the host, network applications running and more.

Evidence MUST be gathered in a manner detailing every action performed on the computer or network system. The IIC is responsible for collection of evidence during an incident investigation. All pieces of evidence should be itemized with the minimum following information recorded.

1. Evidence tag number.
2. Evidence description.
3. Time (including UTC offset) and date discovered.
4. The full name and title of any person(s) who handled the evidence.
5. Storage notes and details regarding the security of such storage.

Information resulting from interviews with personnel should be verified for accuracy. Care should be taken to preserve access, modification and change times on all data. Notes regarding the incident MUST include the date and a signature, per page. Electronic notes and records should be prepended with a timestamp and be digitally signed. Thorough notes should be kept of all actions taking place in evidence collection; include the time and date of all actions, and the executors of such actions. More information on evidence collection is detailed in the next section.

7.7 Forensic Analysis

The forensic discovery and analysis should attempt to answer the following questions.

1. Who the perpetrators and victims of the events were.
2. What events took place.
3. When the events occured.
4. Where the events occured and what they affected.
5. How the events occured.

The examiner MUST disclude proprietary and confidential information unless it directly influenced events of the incident. This discrimination is required as the analysis and testimony of the examiner may be disclosed to defense counsel and general public. Data should not be obfuscated if it directly impacts the a successful report and analysis.

Analysis of the evidence should be performed deliberately and free of distraction. The examiner MUST perform their analysis impartial, and free of presumption. Each step in the analysis should be documented and include the date and time of the action.

The examiner should be prepared to testify in a Court of Law as to the actions performed during investigation. The examiner should be capable of describing, in detail, the utilities used for forensic analysis, how they work, the results of such actions and the impact this evidence may have on other pieces of evidence analyzed.

The examiner should prefer to conduct the examination in a secure, trusted environment; this may require moving evidence. Prior to moving the evidence, the examiner MUST note, and where possible photograph, evidence including serial numbers, asset identification, time of departure from the crime scene, transport time of hardware, arrival time, transport routing numbers, name and title of all handlers of evidence and analysis location. During all changes of custody, this information MUST also be recorded. Where possible, time coded video of the crime scene, transportation of evidence and analysis should be created.

If a computer is to be seized its peripheral components, including keyboard, mouse, external storage drives, network cables, power cables and supplies, etc., MUST be seized. Further, all seizure MUST comply with University, local, state and federal laws. It is necessary to consult with Law Enforcement agencies when the scope of seizure exceeds the authority and accessibility of the examiner.

Investigating an incident involving intrustion may require the examiner to perform analysis while the host is still in a “live” state. When analyzing in this manner, statically compiled utilities should be used. These tools should reside in the examiners toolkit.

File analyses should occur against bit-stream images of media. Utilities used to make bit-stream image copies MUST NOT modify the access, modification or creation times of the media; use cryptographic checksums prior to copy and verify the copied media. All media used to retain the copies of evidence should be properly sterilized by degaussing the media and/or performing low-level formats of the media. Place the original evidence media in plastic bags, label the evidence and store them in a secure location.

7.8 Close Investigation

The IIC and IL, in conjunction with the Incident Response Team, should determine a closing date for the investigation. Investigation efforts MUST suspect aft such closing

date.

7.9 Incident Follow-Up

Incident follow-up should only occur, when required, by University, legal, state and federal authorities.

7.10 Final Report

7.10.1 Information to Include

A final report should be delivered to University authorities. This report should contain the following measures.

1. Copyright statement.
2. Document classification.
3. Distribution list.
4. Executive Summary.
5. A detached digital signature of the document made with an identity strongly embedded in the Web-of-Trust.

Data gathered during the incident investigation, and all forensic analysis discoveries, should be included in the final report.

7.10.2 Storing the Report

All evidence and reports MUST be housed in a secure location and may be archived onto secure media.

7.11 Preventing Future Incident

The Incident Response Team, in conjunction with the Information Security Team, should report any recommendations for future prevention of incidents. These recommendations should be detailed in a seperate document and not include any reference to the original incident. A policy or “best practice” should be drafted to ensure a guideline be available to the University.

8 Acknowledgements

Portions of this document have been influenced by the research and development of Dominique Brezinkski and Dave Dittrich, information security and incident response experts. The author wishes to extend a warm appreciation to these individuals.

References

[1] Webster's Revised Unabridged Dictionary
C. & G. Merriam Co.
Springfield, MA. 1913.

[2] Key Words for Use in RFCs to Indicate Requirement Levels
Request for Comments No. 2119
Bradner, S., The Internet Engineering Task Force, March 1997.