Incident Handling:
An Orderly Response to Unexpected Events

Richard L. Rollason-Reese
Eastern Connecticut State University
83 Windham St.
Willimantic, CT 06226
1-860-465-5298
reese@easternct.edu

ABSTRACT

Computer viruses, worms, denial of service attacks, equipment failures, vandalism, theft and other unwelcome events can send your computer services staff scrambling and cause a variety of problems for your user community. Even the least of these situations can be a distraction for your staff. The most severe can provide an unscheduled opportunity to test your disaster recovery procedure! How does your organization react to these events? Do you have a clearly-defined process in place to deal with unexpected incidents that threaten the security or operation of your systems?

Eastern Connecticut State University is a public liberal arts institution with an enrollment of about 5000 students. Our Information Technology Services (ITS) group has implemented a process that provides a framework for an orderly response to unexpected events. The process is an adaptation of security incident response recommendations from the National Institute of Standards and Technology, Internet Security Systems, Inc. and other resources, which have been tailored for our institutional needs. At the core of the process is the Incident Response Team, which consists of a team manager, a technical leader and other ad hoc team members, depending on the nature and severity of the event. The team concept takes advantage of institutional expertise from law enforcement, human resources, audit, public relations, facilities management, legal services and other technical resources within ITS. The team manages information gathering, analysis, recovery and administrative functions to ensure a controlled, coordinated approach to incident response.

Our presentation will focus on the phases of the incident response process and the role of the Incident Response Team. Flexibility, wise use of resources, effective communications and analytical skills are contributing factors to a successful response effort. We will draw upon our own experiences in discussing communication with the user community, severity level guidelines, evidence gathering, essential documentation, and lessons learned along the way.

SIGUCCS 03, September 21-24, 2003, San Antonio, Texas, USA.

Categories and Subject Descriptors

K.6.1 [**Management of Computing and Information Systems**]: Project and People Management---*management techniques, staffing*; K.6.5 [**Management of Computing and Information Systems]**: Security and Protection.

General Terms

Management, Security.

Keywords

Incident handling, incident response, response team, emergency, attack, recovery.

1. BACKGROUND

Threats to computer security and integrity are not limited to government agencies or corporate giants. Any college or university with a network link to the outside world assumes a significant level of risk. The rate of computer security incidents continues to increase dramatically. The number of incidents reported to the CERT® Coordination Center climbed from 52,658 in 2001 to 82,094 in 2002, a 55% increase in one year [1].

The possible sources of security threats are nearly limitless and can be internal or external. Vulnerabilities can take many forms, some of which are disturbingly common and close to home: unprotected servers, missing keys, unlocked doors, compromised passwords, disgruntled employees or inquisitive students.

Without a crystal ball, it is impossible to predict, with complete accuracy, the nature or timing of future incidents. Prudent planning and technical expertise can minimize, but not eliminate vulnerabilities.

2. THE PLAN

The occurrence of unexpected events may be inevitable, but their effect can be mitigated by the implementation of an incident handling process. The purpose of this process is to provide a framework for an orderly, coordinated response by appropriate resources within the institution.

The National Institute of Standards and Technology (NIST), in a 1991 publication, argued that significant changes in the computing environment require a different approach to security. Four factors were identified as contributing to increased risk of exploitation: an emphasis on confidentiality of data, the growth of local and wide area networks, the proliferation of personal

computers and increasing system complexity [2]. While the emphasis of traditional protection efforts was on physical security and backups, a proactive approach is now required to enable a rapid and efficient response to unexpected events. NIST recommends that organizations establish a Computer Security Response Capability (CSIRC), a process that provides centralized response and reporting functions for security incidents.

Internet Security Systems (ISS) also advocates for the creation of a Computer Security Incident Response Plan (CSIRP.) At the heart of this plan is the Computer Security Incident Response Team (CSIRT), which consists of a team manager, a management advisory board and other permanent and temporary team members [3]. Temporary members provide expertise on technical, business, legal or administrative issues, as determined by the nature and scope of the incident.

Eastern Connecticut State University has adapted these recommendations to define a process that is thorough, yet flexible enough to be used in a small liberal arts institution. Our implementation takes advantage of institutional expertise, both inside and outside ITS, without additional personnel or funding. The team approach is not meant to take the place of a dedicated security staff person with responsibility for planning, analysis, monitoring and reporting on a daily basis. However, this person would be a likely candidate for response team membership.

We have also expanded the definition of "incident" for our purposes, to include *any event that may threaten or compromise the security, operation or integrity of computing resources*. Our team has responded to such diverse events as network probing activities, burst sprinkler pipes in a computer lab, email service interruptions and equipment theft. In each of these cases, the process provided the framework for an organized response, the appropriate allocation of resources, communication of accurate information to the affected constituencies and concise documentation and reporting.

There is value in using the word "incident" to describe any event that requires the response team's attention. Terms such as "hacker" or "attack" may invite sensationalized publicity or unwarranted apprehension within the organization.

3. THE TEAM

The core of the Incident Response Team (IRT) consists of two designated ITS staff who function as the *team manager* and *technical leader*. Backup personnel for these positions are identified to function in the absence of designated staff.

The team manager coordinates efforts of the team members, provides status information to the Chief Information Officer (CIO) and other senior management, and calls on expert resources outside of ITS as the situation warrants. The person who assumes this role should be familiar with computer security issues, the function of ITS areas and staff, general university operations, as well as the role of other personnel in the institution who may serve as resources for the IRT. The team manager must be able to coordinate the efforts of other team members under demanding circumstances and to deal appropriately with situations that require tact or confidentiality.

The technical leader contributes to an assessment of the nature and severity of an incident, advises the team manager on security control and recovery issues, and calls on additional technical resources as needed. Ideally, this person will have a detailed understanding of operational and systems security as implemented at the institution.

Other personnel are added to the team on an ad hoc basis and remain team members until the incident is closed. Depending on the situation, these additional resources may be required to serve functions such as: law enforcement, legal, audit, human resources, public relations, facilities management or IT technical specialties.

4. THE PROCESS

If unexpected events are, by definition, unpredictable, how does the Incident Response Team prepare? Certainly, relevant technical knowledge and managerial experience are prerequisites for the core team members. But the team must have a consistent, multi-phased process in place that will provide guidance in a variety of situations [4].

The response process must provide for (1) a rapid, initial assessment of the extent and severity of the threat (2) coordination with expert resources in law enforcement, public relations and other areas, as needed (3) effective technical action to prevent, counteract or recover from the threat (4) confidential research and evidence gathering (5) thorough documentation and (6) efficient status reporting to management.

Eastern's response process consists of five phases: Alert, Analysis, Response, Recovery and Maintenance.

4.1 Alert

In this phase, the IRT learns about a real or potential threat to security. The initial report may come from firewalls or other detection systems, virus protection software, recipients of threatening emails, security organizations or other sources. The team manager is notified and then contacts the resources required for the Analysis phase, beginning with the technical leader.

It is essential that all university employees be informed about the purpose of the Incident Response Team and the incident reporting process. They should know who to contact and how to reach them. At Eastern, our Chief Information Officer issued a university-wide email to announce the formation of the team and provide a summary of the process. Certain university personnel, such as campus security officers or lab managers, who may be the first to hear of relevant incidents, should be instructed to contact the team manager as soon as it is practically possible.

4.2 Analysis

It is the Analysis phase that lays the groundwork for actions taken later in the process. The decisions made at this time can make the difference between control and chaos. If the onset of the incident is imminent or already in progress, a quick, but informed decision may be required to prevent further damage until a more thorough response plan can be developed.

The first issue to address is whether or not the event is a bona fide threat. The team manager and technical leader examine the information provided by the person, system or organization that reported the incident in order to determine whether the report is genuine. Does the information come from a trusted source? Can it be verified or corroborated?

If the event is genuine, does it qualify as an incident? The answer may be obvious if critical systems are down, your firewall is screaming for attention, the email server is being flooded or there is smoke pouring from a communications closet. Other situations

may not be as clear cut, especially when first suspected or reported. When in doubt, refer to your organization's definition of "incident" and tap your team's collective knowledge and experience. Were there any similar prior events that established precedence?

The next step is to determine the severity level of the threat or impact. Table 1 lists the severity levels in effect at Eastern. The number of levels and their criteria can be tailored to the needs and priorities of the institution.

Table 1. Severity Levels

Level	Category	Criteria
1	Extreme	Emergency situation – poses a threat to the entire university computing infrastructure
2	Critical	Poses a threat to the integrity or operation of critical university systems or network resources
3	High	Threatens one or more applications or facilities that are integral to daily university functions
4	Medium	Presents a risk to isolated, non-production university systems
5	Low	Presents low risk due to minimal exposure or ineffective nature of the threat

Additional expert resources from law enforcement, human resources and other areas may be called upon to assist with the analysis, as needed. These resources may continue to function as ad hoc IRT members until incident response and recovery have been addressed.

If the incident appears to be an intentional attack from external sources, the institution must decide whether to pursue the perpetrator before crafting a response. Attacks from internal sources are handled in accordance with applicable university policies. In either case, it is important to consult your law enforcement or human resources staff before proceeding.

4.3 Response

If the initial analysis indicates that there is an imminent or ongoing threat, "triage" actions may be taken in proportion to the severity level of the incident. Measures may have to be taken quickly to avoid damage to university resources or further escalation of the problem.

In this phase, IRT members perform research and collect materials (logs, emails, files) relevant to the incident. In the case of an intentional act, if the university has decided to pursue the perpetrator, care must be taken to gather materials and information in accordance with established forensic practices. Evidentiary materials must be stored in a secure location to prevent loss or tampering. Consult your institutional legal advisers or law enforcement personnel for their recommendations. In the case of potential criminal activity or violation of institutional policies, information and materials collected must be treated as confidential by all team members. After the relevant materials have been gathered, IRT members assess the impact of the event, including verification of the severity and extent of damage and develop an appropriate response procedure. The team manager may determine that consultation with the CIO, senior management or other resources may be necessary before responding.

4.4 Recovery

The objective of this phase is to restore all affected systems to their proper operational state. Recovery efforts may require network or system downtime. If so, the severity of the situation must be taken into account before scheduling service interruptions. Recovery tasks may include execution of anti-viral cleanup procedures, reconfiguration of systems, restoration of files or systems from backup tapes, modification of criteria on firewalls and other security systems or the application of patches or updates to operating systems or other software.

In the case of severe physical damage, equipment replacement may be required. Disaster recovery procedures may also be invoked if senior management determines that such action is warranted. This is especially true if major systems are likely to be unavailable for a significant period of time and alternative means of carrying on university business must be identified.

4.5 Maintenance

In this final phase, the IRT has the opportunity to reflect on the steps taken to respond to this incident and identify strengths or weaknesses to be considered in response to future incidents. Additional preventive measures may also be recommended as a follow-up to the incident. If so, these recommendations should be noted in the relevant section of the report described below.

When response and recovery activities have been accomplished, the team manager will submit a completed copy of the incident report to team members and other interested parties.

5.0 DOCUMENTATION

Throughout the process, the team manager or other designated team member should keep a file of relevant activities, decisions and evidence gathered. This may include alerts from security organizations or product vendors, statements from affected individuals, error logs, network traffic analyses, equipment inventory lists, damage assessments, email messages and attachments, correspondence with external organizations or any other materials that contribute to a complete and accurate record of the incident and the institution's response.

Essential details should be recorded in an *incident report*. The format of the report can be designed to serve institutional needs. It should be brief and to the point. Evidence and other supporting materials, as cited above, should be included as attachments to the report. Public institutions should be aware that the report and other collected materials may be subject to scrutiny under your state's Freedom of Information Act.

The sample report (Figure 1) represents the format in use at Eastern and records the following information:

North Pole State University

Incident Report

Incident Number: 2003-014

Date of Incident: 2/12/03

Type of Incident: Network Intrusion

Severity Level: High

Response Team Resources: S. Nicholas, Manager
R. Smith, Technical Leader
T. Jones, Technical Resource
F. Garcia, Housing Representative
C. Anthony, Housing Staff

Incident Status: Closed

Date Incident Closed: 2/17/03

Report Filed by: S. Nicholas

Date Report Filed: 2/19/03

Report Distributed to: G. Patterson, CIO
F. Garcia, Housing Director
R. Smith, Network Manager

Description of Incident: On 2/12/03 our network intrusion detection system reported a high frequency of probes (port scans) being sent from a computer within NPSU's network.

Investigative Procedure: Mr. Smith determined that the probing activity was coming from a resident student PC in Room 227 of Tundra Hall. Mr. Smith notified Ms. Garcia in Housing that the network jack in that room had been disabled as of 2/12/03, pending further action. Ms. Garcia contacted Ms. Anthony, the Tundra Hall Director, and asked her to identify the owner of the computer and have them get in touch with Mr. Smith.

Findings: Ms. Anthony identified the computer owner as George Bailey. Mr. Bailey contacted Mr. Smith, who made an appointment to examine his computer. Mr. Smith found that a "spyware" program had been installed on the computer, probably through one of the popular peer-to-peer applications. The computer owner had agreed to the installation of some software on his computer, as promoted by one or more of these applications. The spyware program was attempting to probe a range of addresses within the domain of a commercial services provider. Mr. Bailey appeared to be unaware of the nature of these programs or that they engaged in probing activity.

Resolution: The spyware had made some significant configuration changes in the computer in an attempt influence usage patterns of the user. Mr. Smith and Mr. Jones spent a significant amount of time attempting to remove the spyware from the user's computer because the software did not provide a standard deinstallation procedure. A customized deinstallation procedure was obtained from a source on the Internet and the spyware was successfully removed.

Impact on Current Systems: One student-owned computer was compromised by the installation of spyware. Probing patterns were detected on our network by an intrusion monitor, although it did not have a significant impact on local network performance. The severity rating was classified as "High" because of the potential for disruption of network services and the liability presented by such activity originating from within our network.

Recommended Actions: Mr. Smith tested a freeware program that attempts to locate and clean spyware. If this proves to be a trustworthy and reliable program, we may want to recommend it to our users, especially students. Our CIO also recommended that we take some action to increase awareness of this issue among the students.

Figure 1. Sample Incident Report

Incident Number and Date – Our number consists of the year and a sequentially assigned number.

Type of Incident – These are categories defined by the institution. Examples include: virus attack, equipment failure, unauthorized access, service interruption.

Severity Level – This is determined by measuring the known or perceived threat against the criteria established. The severity level may be modified as the situation evolves.

Response Team Resources – All personnel who participated in the response process for this incident are listed, along with the function they served within the process.

Incident Status (Open/Closed)/ Date Closed – "Closed" indicates that the Recovery phase of the process is complete. Further cleanup or enhancements may be pending, but functionality has been restored.

Report Filed By/Date Filed – Typically, the report is written and filed by the team manager.

Report Distributed To – In our implementation, a draft of the report is circulated to team members for corrections and comments. Final reports are distributed to the CIO, selected team members and managers in the university community whose areas were affected.

Description of Incident – This is a brief statement that describes the incident, in general. Details will follow in other sections.

Investigative Procedure – Provide detailed information about who was involved with the Analysis phase and the methods and resources they used to investigate the incident.

Findings – Describe the results of the Analysis phase. What was the source of the problem? Which systems or resources were affected and to what extent? Were vulnerabilities identified that contributed to the problem?

Resolution – This is the place to describe actions that were taken in the Response and Recovery phases. Details documented here may become a valuable resource for responding to similar incidents in the future. Recovery recommendations obtained from other sources should be referenced here and appended to the report.

Impact on Current Systems – Describe, in general terms, the impact on the institution's systems. Examples: registration activities were interrupted; the primary student computer lab was closed on Tuesday; network print services were unavailable for a 2-hour period.

Recommended Actions – Document configuration modifications, upgrades, procedural changes and other recommendations from the Maintenance phase of the process. If you are still vulnerable to similar threats, recommend preventive measures that can be taken.

6.0 HINTS AND OBSERVATIONS

There is no more effective teacher than experience. Less than a year after implementing our incident response process, Eastern's team has already learned valuable lessons. We offer the following hints and observations.

Motivation

Why did Eastern decide to implement an incident response process? In general, the motivation was a matter of control. This process encourages better decision-making by replacing anecdotal information with accurate reporting. It also captures organizational history and collective knowledge, which, in turn, provides a means of tracking trends and identifying vulnerabilities. It is already clear that this process will provide us with these advantages.

Don't Procrastinate

If you don't already have a response process in place, now is the time to create one. The typical university or college computing environment is more open by design and therefore, is more vulnerable than most commercial environments. A variety of legislation in recent years compels us to place a higher priority on the privacy and security of our systems. [5]

Time Well Spent

Time commitments to incident response will vary as needs arise, especially for the team manager and technical leader. The time and effort spent in establishing an incident response process will yield a more efficient and controlled operation in the long run.

Spread the Word

University personnel should be reminded periodically about the existence and purpose of the Incident Response Team. Provide them with contact information. Let them know that you are prepared to respond when needed. An introduction to incident response practices should be a component of the orientation process for new IT personnel.

Refine the Process

As you put the process into practice, you may find aspects that need to be adjusted for your environment. It may take some time to clarify the scope of your efforts. Where do you draw the line between day-to-day issues and incidents that deserve more focused attention? Fine tune the process to address your needs more effectively.

Know Your Experts

Before implementing the process, identify those resources in your campus community who are likely to be asked to join the team as permanent or ad hoc members. Talk with them about the process and the value of their contribution.

Stay In Touch

Effective communication among team members is crucial throughout the process. Provide periodic status information to the university administration and public relations staff, if the incident is likely to draw media attention. Keep a tight rein on confidential information.

Assess the Results

Use the information in your incident reports as an assessment tool. Prepare a report, at least annually, that summarizes the type of incidents addressed, resources used and recommendations for preventing or responding to similar situations in the future. Review your accomplishments and take the time to recognize individuals who have contributed to your efforts!

7.0 ACKNOWLEDGEMENTS

Eastern Connecticut State University is indebted to our Chief Information Officer, George Kahkedjian, without whose guidance our incident response process would not have progressed from concept to practice.

David Bachand, our Network Manager, is the team's vigilant technical leader. His detailed knowledge of networks, operating systems and their vulnerabilities provides our team with a solid technical foundation. We also appreciate the contributions of the other Eastern staff and administrators who have lent their institutional expertise to our cause.

8.0 REFERENCES AND RESOURCES

[1] "CERT® /CC Statistics 1988-2003." Carnegie Mellon University Software Engineering Institute, CERT® Coordination Center. <http://www.cert.org/stats/> (3 July 2003).

[2] Wack, John P. "Establishing a Computer Security Incident Response Capability" (Special Publication 800-3). NIST Computer Security Resource Center - CSD, November 1991. <http://csrc.nist.gov/publications/nistpubs/> (3 July 2003).

[3] "Computer Security Incident Response Planning: Preparing for the Inevitable." Internet Security Systems, Inc., 2001. <http://www.iss.net/support/documentation/whitepapers/technical.php> (3 July 2003).

[4] "Computer Security Incident Response Planning: Preparing for the Inevitable." Internet Security Systems, Inc., 2001. <http://www.iss.net/support/documentation/whitepapers/technical.php> (3 July 2003).

[5] Wada, Kent. "IT Security on Campus: A Fragile Equilibrium." Syllabus, Vol. 16, No. 10 (May 2003), 17-20.

Other helpful resources:

"An Introduction to Computer Security: The NIST Handbook" (Special Publication 800-12). NIST Computer Security Resource Center – CSD, October 1995. <http://csrc.nist.gov/publications/nistpubs/> (3 July 2003).

Swanson, Marianne and Barbara Guttman. "Generally Accepted Principles and Practices for Securing Information Technology Systems" (Special Publication 800-14). NIST Computer Security Resource Center – CSD, September 1996. <http://csrc.nist.gov/publications/nistpubs/> (3 July 2003).

Swanson, Marianne. "Guide for Developing Security Plans for Information Technology Systems" (Special Publication 800-18). NIST Computer Security Resource Center – CSD, December 1998. <http://csrc.nist.gov/publications/nistpubs/> (3 July 2003).

"Creating a Computer Security Incident Response Team: A Process for Getting Started." Carnegie Mellon University Software Engineering Institute, CERT® Coordination Center, 2002. <http://www.cert.org/csirts/Creating-A-CSIRT.html> (3 July 2003).