Global Information Assurance Certification Paper

Incident Handling: A Case Study in a University Department
GSEC Version 1.3
April 23, 2002
Tom Tsubota

Introduction.

In this document, I will describe the process I used to respond to a security incident. The incident that had occurred involved a former manager who attempted to use our computer system to obtain information against our university department. Coincidentally, this incident had occurred not too long after I attended training in the SANS Security Essentials. This provided me the opportunity to refer to materials from Eric Cole's "Incident Handling Foundations"(1) from the SANS Security Essentials courseware. From Cole's materials, I had relied on the "six steps" in incident handling to help me organize my approach to handle the incident. In this document, I will describe how I proceeded to handle the incident based on the steps from the SANS material. These steps are preparation, identification, containment, eradication, recovery, and lesson learned. I will describe in this document how I handled the incident following these steps and the lessons learned from the experience.

Preparation.

The preparation phase involves the establishment of policies and procedures to effectively deal with the incident. These are usually prepared in advance to provide the system administrators guidelines on how to deal with the incident. By having policies and procedures organized and accessible to everyone, system administrators can minimize the chance for confusion and errors in the incident handling process.
As an example from the Department of Commerce's website (2), their policy and procedures are based on the "Incident Handling six steps"(1) and made them available on the web for easy access. In addition, we could also resource more information on incident handling from the Federal Computer Incident Response Capability (FedCIRC) and the SANS Institute website.

Management should play an important role in supporting the policies and procedures. Without this support, management would not understand your responsibilities for protecting the computer systems or worse employees would not take it seriously. The system administrators should take responsibility in advising the management of the policies and procedures. As for the management, "they do not have to understand how it works, but they need to be involved to ensure that the business processes are protected and not hindered by security decisions."(4) Both entities should understand the goals of implementing the policies and procedures.

Unfortunately, I quickly realized that we do not have these policies in which our management can refer to for this incident. Without a policy, it was difficult for management to understand what the IT staff's responsibilities are for handling incidents. Our management had started to realize the potential political harm this incident would cause them. I had to spend some time with my supervisor to explain to management how IT will deal with the incident and have them agree to it. In addition, my co-workers and I had not established a set of procedures for handling incidents. This would be important to ensure there would be order to the investigation and avoid unnecessary confusion. Unfortunately, since we had not established this, it proved to have poor results. Every one of us attempted to be helpful in dealing with the incident, but as a result my co-workers unknowingly began to tamper or taint the evidence. One of my co-workers had proceeded to access the property options and even opened some of the files. As a result, his investigative attempt affected the chance these files can be used as evidence. I had realized it was important to preserve the rest of the evidence in order to continue working on the incident. It can be stated that, "if you don't take care of your evidence, the rest of the investigation will be compromised."(8)

With that in mind, I had to step in to stop everyone from doing further damage to the evidence and had my supervisor grant me the authority to the investigation. I also had to ensure my supervisor I will be following the SANS incident handling steps as best I could and communicate to him my progress in handling the incident. Even though I was successful in gaining confidence with management for dealing with the incident, I became the only incident handler. This made dealing with the incident easier without the interference. Even though, I had in the end resolved the incident, I still found myself at a disadvantage to handling this incident. The following section from Moira West-Brown article, "Avoiding the Trial-by-Fire Approach to Security Incidents,"(5) illustrates examples of the disadvantages I faced handling the incident. At each step, I will describe how each of step relates to my incident handling experience.

- *Serious intrusions may still go undetected.*

  This was true for this incident. My co-workers and I would not have detected this incident, if the director had not notified us.

- *Volunteers may be able to deal with the technical issues, but may not understand or have the information available to assess the business consequences of any steps taken.*

  I clearly did not have the understanding or time to realize the consequences. Most of this I had to rely on my supervisor based on his management experience.

- *Volunteers may not have the authority to apply the technical steps (e.g., disconnecting the organization from the Internet) or other actions they*

believe are necessary (e.g., reporting the activity to law enforcement or seeking the advice of legal counsel).

My supervisor had to exercise this role to authorize the technical steps I needed to take for this incident. We also felt we did not find it necessary to report this incident to law enforcement.

- *There may be delays in seeking and obtaining management approval to respond.*

  I had experienced delays in obtaining management approval to act on the incident, mostly due to inexperience and lack of realizing that there was a problem.

- *Volunteers have no "bigger picture" of the overall detection and response activity.*

  This was true for the first time we had to recognize this incident and that my primary means of reference were my SANS course materials. The materials were used as a guideline to help formulate a procedure for incident handling.

- *Volunteers may know in some cases who to contact internally, but anomalies may exist.*

  Even though, I felt I did my job knowing whom to contact, I was still uncertain to whom I needed to reveal this information to.

- *Other individuals in the company who identify a possible security incident may not be aware of the informal group and may fail to report to it.*

  Most individuals in our department just assume the IT group just keeps the computers running and will always fix the computers whenever it is not running correctly.

- *An informal group is unlikely to have external recognition and support.*

  For our IT group, it was assumed that this incident was as simple to resolve as any troubleshooting event.

Identification.

This phase involves the determination of whether or not the event that occurred is an incident. An incident can defined as “an adverse event in an information system and/or network or the threat of the occurrence of such event” (3). Examples of these events can include malicious code attacks, unauthorized

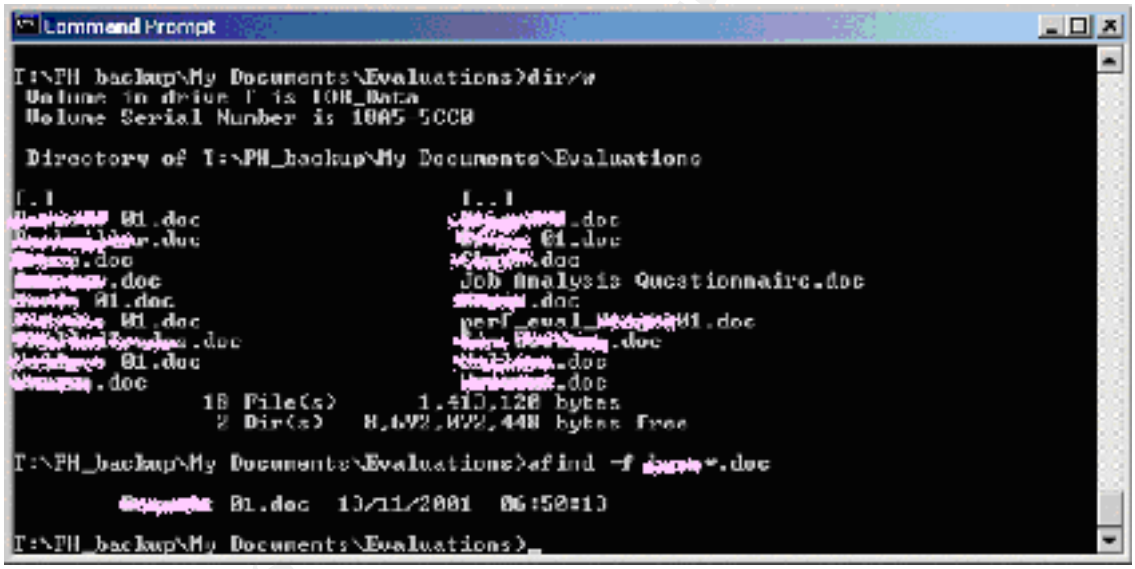
access, denial of service, and misuse of computer systems. In addition, fire, natural disasters, and power outages can also be classified as examples of incidents too. For the purposes of this document, the incident will be defined as an adverse event relating to information security.

In this incident, we see that the event involves unauthorized access to files and the misuse of the accessed files. The incident started one morning when our assistant director entered into the office with a concerned look on his face. He quickly explained to my co-worker and myself about a manager out on mandatory leave from work was somehow able to access his own performance evaluation from the network. The director was quite concerned since this manager filed a complaint with human resources. The manager had already divulged some information to human resources in which only the director knew it could have come from the performance evaluations he had written. The manager attempted to use this information to his advantage as evidence for his grievance claim against our department. The director was in a compromising situation where he may have to explain to human resources about the sensitive information they received from the manager. Obviously, he was very upset that his confidential information had been accessed without his permission. The director wanted us to find out how he had access to his confidential documents, when were the files accessed, and where did the manager get the files. He also wanted a complete report on this before the end of the day.

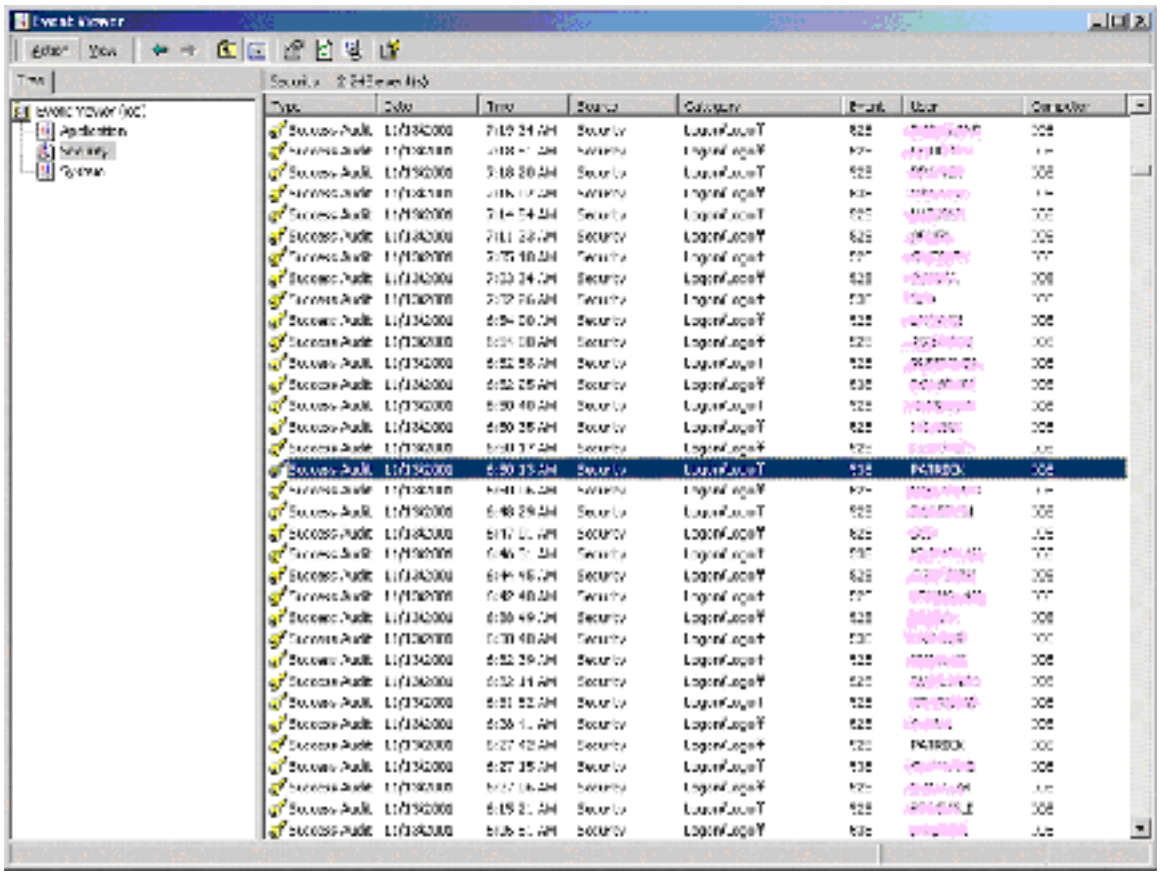
One important step I took was to calm the assistant director. At this point, the incident has raised everyone's stress levels. Staying calm is key to attempting to make an assessment of the incident that occurred. To help this, I had contacted our IT manager to help with the situation. He was able to help calm the director and establish the expectations of how we would resolve this incident. I began asking the director what was accessed, who accessed them, and when it was brought to his attention. This will give me useful clues to give direction on how where I should start on the investigation. In this case, he was able to tell me the files accessed were his performance evaluations that he had formatted in Microsoft Word documents. He was able to give me a list of the names of the Word documents. He then tells me the person that he suspects had accessed the files was one of the managers out on leave and gives me an idea of the manager's intentions for accessing these documents. I was fortunate to find out the manager was last seen at the office one morning when he was suppose to be on leave from work. This fact was also noted to human resources and proved further useful to them when it was complimented with the results of the investigation. I will go into more detail how this was done.

I had found that the documents in question were located in one of the mapped network drives on our Windows network. It was determined that the files were mistakenly copied to the network drive as a backup from the director's computer. The problem was that it placed in a public area and then neglected until now. Clearly, this was an example of an issue for not having a security policy.

After locating the files, I began to gather the evidence. As I mentioned before in this document, my task for gathering evidence became a big challenge after knowing my co-workers had tampered with some of the evidence. I left the tampered files alone and focused on the rest of the files that were not examined. I began searching on the web for forensic tools in which will help me gather the evidence from these files. I chose Windows command-line utility called afind, which I downloaded from http://www.securityfocus.com/tools/525. This utility can determine who had accessed the documents and when they accessed them without modifying the date stamp as you would if you directly accessed the file to look up the file properties. I was able to determine that the documents were accessed at around the same time the manager was last seen at the office during the morning. I took screen shots and pasted them in a document as evidence in which I will provide to management as a report. Unfortunately, the afind utility also confirmed my co-workers had also tampered with some of the other documents. The time stamp has been changed to the time they had touched the documents.



So far the document only shows the time the manager could have access the document. After that I needed to prove that the manager had logged onto the department's computers to access these documents at that time. I then referred to the Windows NT Event Viewer from our domain controller and checked the access logs for anyone who logged in to access the documents at that time. For our Windows network, we had set our auditing policy to log both success and failure logins. I was able to determine the manager had successfully logged in the network on that morning. I also took screen shots of the logs as more evidence to my report. I could also have the security logs exported to an Excel spreadsheet, but I wanted to report information.



So now I was able to determine whom, what, and when, but I still find out where. Everyone had assumed this manager must have used his computer in his office to access the files, but we didn't know, because he had his office door locked. My supervisor assumed it would be OK to gain access to his office from someone who had a key and examine the manager's computer. This proved to be the wrong thing to do, because I had found out from management it would require permission from an authorized human resources representative to grant physical access to the office. The representative can ensure we are not violating any policies (i.e. privacy) during the investigation (5). We could have been held liable for illegally entering a locked office without proper approval from human resources and management. Under guidelines from the Department of Justice (6), we would have to respect this manager's fourth amendment rights and not search the computer. In order to legally search the computer, law enforcement would have to be involved and a legal search warrant would have to be obtained to allow access to the computer.

Going against my supervisor's orders, I chose not to enter the office and continued to look for more evidence from the server logs. After a closer look at the logs, I had found out that the manager did not use his computer to access the documents. From the event viewer logs, I was able to determine the manager had logged into one of his staff's computer and the time stamp closely matched

the time stamp the manager accessed the files. I took screen shots of log event as evidence for my report.

At this point, I lacked the approval from management to confiscate the computer to look for more possible evidence there. Since we lack the policies and procedures, management could not determine if they wanted the responsibility to take ownership of the computer.

Containment.

The purpose of the containment phase is to make sure the incident can be contained and keep it from getting worse. This should involve making backups of compromised systems. At this point, we should determine the need to disable access or to pull systems off the network.

At this phase, I had to make sure that the incident could not get any worse than it was already. With approval from my supervisor, I proceeded to make sure to secure the area by disabling all user access rights to the file directory that contained the suspect files. That way I can ensure no one else may attempt to illicitly access these confidential files. I immediately disabled access to that mapped drive from all users. I then instructed my co-workers to inform the users that part of their access will be temporarily inaccessible. By isolating the access, I can ensure there will be no interference from anyone while I proceeded with gathering the evidence.

Fortunately, we perform daily backups with updated information on our computer network. This is handy in case I need to restore information that would have been altered or purposely deleted from our network. As for the confidential files, I have made a backup copy onto CD to be stored as evidence. I also proceeded to disable the former manager's account access and changed his password to prevent him from using our computer systems again. Normally this step would be the first thing you do, once you suspect a user is attempting to perform an illegal activity.

Unfortunately, I could not secure the computer system I had suspected was used in the incident. Due to the lack of management support, this procedure could not be performed. The computer could have contained potential evidence that could have been used in my report.

Eradication.

The eradication phase basically means that we fix the problem so that it does not happen again. Before the problem could be fixed, we would need to determine the cause of the incident. We then could apply a solution and check to see if this would resolve the issue.

For this phase, I would have determined the best way to resolve the incident before I re-activate access to our users. For this I need to ask the manager's permission to remove his confidential files off of the network. Once I do have his permission, I can quickly remove the files. I can also restore his files from backup if the manager finds it necessary to access these files.

Recovery.

After fixing the problem, we can proceed to bring the system back on-line for use again. It would be best to check the system is fine before attempting to put the system is back on-line. Before restoring access, I made one final check with my supervisor and to have him authorize the access back on-line. Once I have ensured all of the confidential files are no longer accessible to users, I can then restore network access to our users.

I assembled the evidence I collected and composed a report on the incident. I sent copies of the report to my supervisor, management and human resources. Human resources now had information from the report to question the manager's grievance claim. Human resources had found out the manager could not clearly state how he got his information in the first place. Sometime later, the manager had dropped his grievance claim and later resigned from his position.

Lessons Learned.

My experience with handling this incident has me realize the need for improvements on how incidents are dealt with in our department. We will need to create a comprehensive plan that includes a policy on security incidents, procedures to organize a response team, and procedures for reporting and handling incidents. We will also need to have management to support this plan.

With the exception of the SANS material, we do not have a clear concept to deal with incidents. No clear procedure or establishment of people who would be responsible for handling incidents. Our IT group will need to understand the procedures and policies that we establish. Over time, policies and procedures should be updated whenever there are future occurrences of incidents. Fundamentally, we should have a policy and procedures for incident response. By having one, it will state what our responsibilities are and what we are liable.

Our IT group will need to organize a response team or determine individuals that would have the primary role in handling incidents. Proper training and communication skills will be important to organize a good response team. A plan should be made to organize individuals to be assigned roles of responsibility. This can be organized by each individual's skills or expertise.
All of this would minimize the risk for errors and confusion in the investigation.

Management support is important to empower the IT Group to apply and enforce the plan. It would not be important for management to fully understand the details of the plan, but it is important how both of these apply to protect and maintain the business processes of the organization. "The success of the plan depends on how well it is understood and accepted by both upper management and the system users. They must all be comfortable with the plan and trust it if they are to support it and follow the procedures"(7). Without this support, IT would most likely be unable to properly resolve incidents, which are political in nature (i.e. disgruntled employee). Management could simply assume the computer systems are fulfilling the needs of the organization until something hinders that (i.e. an incident). When the "process" is disrupted, management expects the IT group to just fix the problem and forget it. It is important for management and IT to work together to not only fix these problems, but to also protect the computer systems and the business it provides.

Reference:

1. Cole, Eric. "Incident Handling Foundations." SANS Security Esssentials II: Network Security. April 2001.

2. Baker, Roger W. "Computer Security Incident Handling memo." 08 July 1999. URL: http://www.doc.gov/cio/oipr/ITSECmemo7-9-99.htm

3. URL: http://www.fedcirc.gov/docs/understanding.html

4. Barman, Scott. Writing Information Security Policies. New Riders. 2002.

5. West-Brown, Moira. "Avoiding the Trial-by-Fire Approach to Security Incidents." March 1999. URL: http://interactive.sei.cmu.edu/news@sei/columns/security_matters/1999/mar/security_matters.htm

6. Kerr, Orin S. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." January 2001. URL: http://www.cybercrime.gov/searchmanual.htm

7. Adler, David. Grossman, Kenneth L. "Establishing A Computer Incident Response Plan." 2001. URL: http://www.fedcirc.gov/docs/82-02-70.pdf

8. Kruse II, Warren G. Heiser, Jay G. Computer Forensics Incident Response Essentials. Addison-Wesley.

9. Brenton, Chris. Hunt, Cameron. Active Defense A Comprehensive Guide to Network Security. Alameda: Sybex, Inc, 2001.

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event