GIAC Advance Incident Handling and Hacker Exploits Track

Practical for Option 1 – Illustrate an Incident

Edwin Covert, CISSP

SANS New Orleans, LA – January 28 through February 1, 2001

Executive Summary 3

Introduction 4

The Incident Handling Process 6

Preparation 6

Identification 8

Containment 9

Eradication 11

Recovery 11

Follow Up / Lessons Learned 13

Recommendations 13

Conclusions 14

Appendix A - Photographs 15

Appendix B – References 16

Executive Summary

This practical concerns an incident that occurred on August 4, 2000 at the Network Operations Center (NOC) of Federal Computer Systems Incorporated (FCSI). On that date, a sprinkler system head exploded during a furniture and equipment move within the FCSI NOC. This event caused concern as the FCSI NOC was a production environment. From the NOC, FCSI remotely and securely manages client networks and infrastructures. They provide "near-real-time" reporting and correction of network faults and outages. Any interruption of the NOC infrastructure would cause a loss of revenue for FCSI.

This practical considers the sequence of events that occurred and the steps that were taken in response to those events. The consideration given is in the context of the six-step incident response process presented by the SANS staff at SANS New Orleans. This conference was held from January 28 to February 1, 2001.

In this practical, the ideas of Preparation, Identification, Containment, Eradication, Recovery, and any Lessons Learned are processed in two parts: firstly, interviews were conducted with the individuals directly involved from FCSI. Secondly, the author provides commentary on the processes utilized by FCSI as they recovered from this incident.

In the end, a conclusion and recommendations are provided to better educated the employees and management of FCSI in not only the specifics of their response to this incident, but also to provide ways to better prepare for any future incidents.

In the interest of full disclosure, the author of this practical is employed as an ad hoc security consultant for FCSI. He interviewed several people directly involved with the incident: MR, the FCSI LAN Administrator; DR, the FCSI Senior NOC Analyst; MD, the FCSI Director of Enterprise Services, and MW, the FCSI Senior Vice President for Corporate Development. Other personnel were interviewed based on the contribution they made to the recovery effort. In order to protect the privacy of the individuals interviewed for this practical, only their initials are used.

Introduction

On August 4, 2000, a sprinkler head in the FCSI NOC from an automatic fire-suppression system broke off when it was hit by furniture being moved by FCSI NOC employees. These employees were attempting to re-configure the furniture and workstations in the NOC to better facilitate the flow of information within the NOC. That flow of information is vital to FCSI for providing superior network management services to its government and commercial clients.

When the FCSI NOC was originally designed and built, a fire-suppression system was installed per local building codes. This system uses water forced through pipes and out a series of sprinkler heads. The sprinkler heads are shaped in such a way as to spray water in a large pattern at a high rate of volume. The NOC furniture consists of three pods (with three workstations to a pod) and three large monitors in front. Additionally, there is a rack of electronic gear on the front right side that controls the audio-visual (AV) equipment. On the back left side is the FCSI National Helpdesk Support Area. This area provides 24 x 7 helpdesk operations to its clients. Figure 1 provides a diagram of the layout of the FCSI NOC.

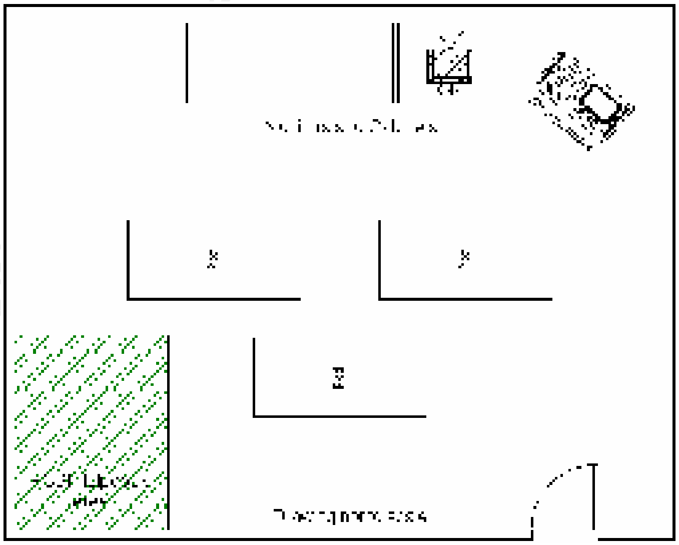

Figure 1 – Floor Diagram of the FCSI NOC

As previously mentioned, in the front of the FCSI NOC are three large monitors. Two monitors are connected via a video switch to the desktop monitors of the NOC Analysts. This allows a supervisor a larger picture of the data that a particular analyst is working on. The third monitor provides a continuous news feed via CNN. The news feed provides critical indications and warnings (I&W) in the event that a situation occurs in an area of the world where a FCSI's client is located. For example, if an earthquake were to occur in California and FCSI had a client in California, the news feed might provide timely information regarding why the network connectivity is down to that client at that particular moment. Each monitor is housed in a floor-to-ceiling storage cabinet. Figure 2 is a diagram of a cabinet that is used to hold the video monitors.

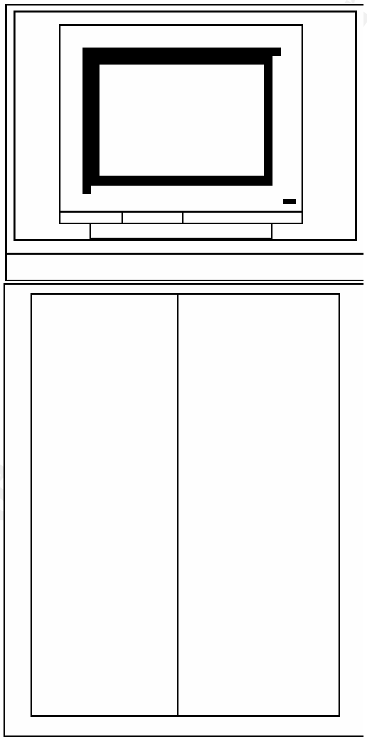

Figure 2 - Monitor Cabinet

Hidden inside the news feed monitor cabinet was a sprinkler head. This sprinkler head came out of the ceiling and through a hole cut in the top of the cabinet. This sprinkler head was unbeknownst to the NOC employees, as it was installed prior to their employment with FCSI. When the NOC employees moved the cabinet that contained the news feed monitor, they inadvertently snapped the sprinkler head from its supply pipe. This action caused an estimated 50 gallons of water to flow from the supply pipe per minute for the next forty minutes. Figure 3 shows a diagram of the cabinet with the location of the sprinkler head.

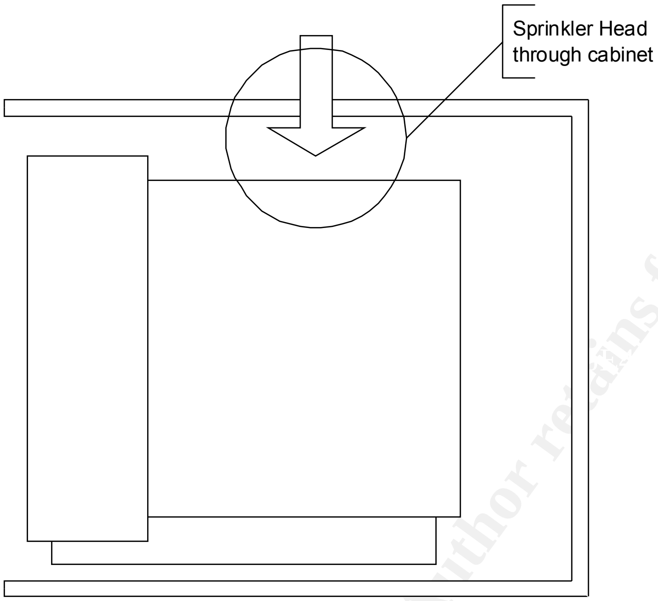

Figure 3 – Sprinkler head in the cabinet (cut away view)

The Incident Handling Process

As explained at the SANS training course for Incident Handling and Hacker Exploits (which the author attended in New Orleans, LA from January 28 through February 1, 2001), there are six steps in the incident handling process. They are Preparation, Identification, Containment, Eradication, Recovery and "Lessons Learned". Each of these steps must be accomplished in order for an effective incident handling exercise to occur.

This practical compares the prescribed six-step process with the specific actions that were actually taken by the FCSI staff (and others). Recommendations for improving the in-house response process follow the narrative in each section.

Preparation

When handling or responding to an incident, preparation is key. Preparation is the idea that a organization is capable of handling an incident when it happens i.e. there is no need to "ramp up". This preparatory capability includes having proper policies and procedures already in place regarding what should occur and who is in charge in the event of an incident. Other items that should be covered in the preparation phase are having the proper tools available and having escalation procedures in place. When most people think of incident handling tools, also called a “jump bag”, they think of the physical items that are used to fix things. A jump bag might contain hardware tools i.e. screw drivers, wrenches, blank media, and system or OS manuals.

Other items can also constitute a tool as well. For instance, knowledge is a tool that can be utilized in the fight against an incident. Escalation procedures (also a type of tool) are those specific policy documents that state who to call when. For example, at what point is the determination made to notify senior management about an incident? Should they even be notified? What about law enforcement? What triggers a “door-knob rattle” vice a criminal act? All of these, and other, issues need to be prepared in advance of an actual incident. Trying to solve or settle these issues at the time an incident is occurring is not a good idea.

If the incident in question is of an illegal nature, extreme caution must be exercised when informing law enforcement: According to Icove et al. (1995), there are four issues that must be understood before an organization calls in law enforcement. They are:

1. Getting approval from upper management. Without upper managements consent and understanding of the situation, there may be repercussions that may not be fully realized at the time.

2. If law enforcement gets involved in a case, they tend to completely take it over. An organization’s internal incident response team will act in a subordinate role.

3. Investigations via law enforcement take time. Resources must be committed to fully explain the situation to investigators. This explanation would include the systems affected; the procedures used thus far, what the organization’s assets and what are the losses involved.

4. Law enforcement is in the business of investigating *and* prosecuting. Therefore, information regarding an organization may become part of the public record. Also, resources need to be committed for appearing in court, testifying, etc.

For FCSI, they had neither an incident-handling procedure nor a documented disaster recovery procedure. This would prove to be a significant handicap later. Also missing from the FCSI toolset was knowledge regarding how the sprinkler system was installed and how it functioned.

Commentary

FCSI made several mistakes before the incident occurred. First and foremost, their security personnel should have instituted both a disaster recovery plan and an incident-handling plan. This simple omission on the part of the security team led immediately to problems.

By not having an incident recovery plan in place (or one that had been practiced a few times) the FCSI NOC staff were left to solve key problems on their own. One of these was "what to do now?" or "who do we call?" As it happens, the author is on the notification list that the alarm company has for FCSI. When the alarm company received an alert that the fire-suppression system had been activated (which was caused by the sudden release of vast amounts of water from the system), the author was notified via his cell phone. As he was in another state at the time, he was of little use. After he confirmed that there was an incident and the FCSI appeared to have the situation under control, his work was done.

FCSI fared better when it came to disaster recovery. MR, the FCSI LAN Administrator, had in place a disaster recovery plan for restoration of critical network servers and workstations. Where he fell short was in the documentation of that plan. His recovery plan was not written down and very few other individuals were aware such a plan was in existence let alone knew how to utilize it in the event that MR was unavailable. According to Russell and Gangemi (1991), a disaster recovery plan should include, among other items, backing up information, storage location (hot, warm, or cold site), retrieval in that stored information and information restoration procedures. As it turned out, there was no need to implement MR's recovery plan. This will be discussed later.

Identification

Identification, as it relates to incident handling, is the concept of noticing a situation and being able to alert others of that situation. In the case of the FCSI NOC, it was immediately noticed that there was a problem based on the existence of water flowing from the cabinet and ceiling. Other employees noticed the ensuing commotion. Emergency evacuation procedures were begun. VS, the Executive Administrative Assistant made an evacuation announcement over the corporate public address system. VS, noticing the liquid had an oily smell to it, also called the local fire department to help identify the exact nature of the water flow. The fire department arrived 15 minutes after being called and began investigating. VS also physically walked through the FCSI spaces to ensure that all non-essential personnel had evacuated.

Commentary

FCSI quickly evacuated the building. This was critical as no one knew exactly was they were dealing with yet. When dealing with a physical disaster, the most important concern is the lives of personnel. Everything else is secondary. Properly calling the fire department (even though they did not know what the source of the problem was yet) was another good action taken by the FCSI staff.

VS, by ensuring that everyone had left the building, could have potentially saved lives. While this disaster ended up being non-threatening in nature, that fact was not known at the time.

Containment

The goal of the containment process is to keep the process from spreading, or getting worse. There are two aspects to containing this particular disaster: keeping the water from spreading into other parts of FCSI and keeping the FCSI personnel safe. DR, the Senior NOC Analyst, attempted to address the second part of this containment scenario by turning off the power to FCSI. He feared what the mix of electricity and the large volume of water flowing from the pipe could cause.

The fire department arrived within 15 minutes of being called. This was an effort to address the first part of the above containment scenario in addition to identifying the source of the problem. They needed to keep the incident from spreading. They surmised the cause of the water flow as being a broken sprinkler head. The oily smell noticed by VS was determined to be residual lubricant in the sprinkler system. They immediately dispatched several crews to begin looking for the water shut-off valve that controls the sprinkler system.

Eventually, the fire department crews located the valve. Even then, when they found the main water valve, it was chained and locked. Bolt cutters were used to unchain the valve and shut off the flow of water into the NOC. However, all of the buildings in the complex where FCSI is located have an interconnected sprinkler system. This meant that the water flowed from the pipes for another 10 minutes as the entire system drained. Once they had ensured that the flow of water into the NOC has completely ceased, the fire department and their crews departed the scene.

As a side note, when the fire department located the water valve, it was in a closet. Placed in front of the closet were several stacks of miscellaneous office articles. VS also called a local electrical firm. They ascertained that the water had not gotten high enough to cause damage to the NOC electrical system. This allowed NOC staff and others to begin plugging in the necessary recovery equipment e.g. wet-dry vacuums, etc.

Commentary

With an unknown physical disaster, the safety of the personnel on-scene is paramount. DR made an excellent decision to shut off the power. However, as will be pointed out later, the manner in which he did this caused another issue to arise. It is important to note that he is not to be faulted for his actions. The pressures at the time of the event dictated his methods.

The situation with materials placed in front of the main water valve is of great concern. The author recently reviewed this detail first hand at FCSI during an on-site inspection and security review. FCSI could potentially be placing its employees' lives in danger with the cluttered valve closet.

There is little to be gained by criticizing the response time of the fire department, as there is no viable means for improving it. While the author would like to have had the fire department arrive sooner, he does not know what other emergency situations they are working on at that time. This same argument can be made for the situation involving the interconnectedness of the building's fire suppression system in the FCSI complex. FCSI is a tenant in the complex and short of relocating, there is little that they can or could do to mitigate this risk.

Eradication

Eradication, as defined in the SANS Incident Handling course book, is the removal of the cause of the incident. In the case of the FCSI NOC and the sprinkler head, the eradication effort was primarily aimed at the removal and replacement of the broken sprinkler head. MW, the Senior Vice President, coordinated this process with a company that specializes in this work. They arrived and replaced the damaged head with a new one.

Had this incident not been a physical disaster recovery incident, but a network intrusion incident, this is the phase of the process where the source of the intrusion would have been removed from the system. This could be a complete reinstall of the operating system binaries and pertinent data (a la 'nuking the system from high orbit', as Stephen Northcutt (1999), says). It also could be subtler. If the source of the incident is a piece of malicious code, for example a Microsoft Word macro virus, the incident handler might simply install or update a commercial anti-virus program. As with any process that involves many variables, the situation at hand would dictate the procedures used.

Commentary

The eradication effort for FCSI, while in theory should have been a distinct process, was combined with the containment effort. It is important to note for the purposes of this practical that these steps are distinct in nature. However, it is suspected that this combination of steps is often the case. Individual steps in high-stress processes often blur, overlap or happen concurrently.

Recovery

As soon as the fire department had left and the "all clear" signal was given that allowed employees back into the facility, MW, the Senior Vice President, organized a basic cleanup effort. He began by sending some individuals to a local home-improvement store for mops and buckets in an effort to remove the standing water in the NOC. Additionally, he gathered a group of employees to begin removing the remaining furniture from the NOC. VS, the Executive Administrative Assistant, called a company that specializes in the restoration of spaces that have suffered fire or water damage. They arrived one-and-a-half hours later.

The recovery process continued for several days. The professional recovery firm removed the remaining standing water. The FCSI NOC staff, led by DR, repainted the NOC and eventually reconfigured the furniture. A carpet company was brought in to remove the existing water-soaked carpet and lay new carpet down.

FCSI spent approximately three weeks cleaning and restoring the NOC. During this time, they were still conducting normal business operations, although at a reduced capacity. FCSI utilized backup physical spaces to continue managing client networks remotely.

If FCSI had not been dealing with strictly a disaster-recovery incident, but rather an intrusion incident, there are other options they could have considered. For instance, in certain situations, FCSI may have chosen to prosecute the offender. There are a number of specific laws against unauthorized access to a computer system. As an example, "The federal Electronic Communications Privacy Act (EPCA) prohibits all monitoring of wire, oral and electronic communications unless specific statuary exceptions apply" (Icove et al., 1995, p. 166).

Commentary

As this was a scheduled furniture reconfiguration, almost all of the network equipment and other computers were already removed from the NOC. This prevented a massive disaster, as the data in the NOC machines was invaluable to FCSI business operations.

The only equipment concern for FCSI was the uninterruptible power supply (UPS) that the NOC used. The UPS needed a precise shutdown routine. When DR quickly shut off the power to the FCSI facility, that routine was not followed. As such, the FCSI NOC staff had to spend 30 minutes or so with UPS vendor reinitializing the UPS and performing recovery schemes. Again, it is hard to fault DR's actions regarding the shutdown. He was attempting to shut off the power to potentially save lives and the 30 minutes spent reinitializing the UPS is a small price to pay for that concern. However, FCSI would have been better served if he the NOC staff had documented the efforts they made to recover the UPS. This would have prevented future recovery teams from having to "reinvent the wheel".

Lessons Learned

The last step in the incident handling process is conducting a lessons learned session. The purpose of this procedure is to examine the actions that were taken, what effect they had and how to improve the overall process. This is conducted after the event because "hindsight is 20/20". Events and actions are clearer without the pressures of the incident upon oneself.

FCSI did not hold a "Lessons-learned" session after the incident.

Commentary

It is imperative that a "Lessons-learned" session be held after an incident, especially one of this magnitude. At a minimum, an "after-action report" should be written that documented the steps taken. This will determine whether or not the appropriate processes were followed.

Recommendations

The FCSI disaster had several areas that could be improved.

1. First FCSI's most critical error was not having either a disaster recovery plan or an incident-handling plan. Because of this omission, a certain amount of chaos ensued. While the FCSI staff performed admirably and certain employees assumed leadership roles, a well-documented incident-handling plan and disaster recovery plan would have minimized this incident. It should also be noted that neither an incident-handling plan nor a disaster recovery plan would have prevented this incident from occurring.

2. Another error on FCSI's part was the lack of documentation on plans that actually existed. This is primarily aimed at the disaster recovery plan. The FCSI LAN Administrator needs to ensure that his plans are written down and that multiple people understand them and are able to execute them in his absence.

3. FCSI, when creating its plans, should document the physical layout of their facilities, noting items such as sprinkler heads, control valves, fire extinguishers, etc. These documents should be checked prior to any activity such as the furniture move that occurred.

4. Having blocking materials in front of the main water valve hindered the containment operation. As was noted previously, FCSI could potentially be placing its employees' lives in danger with the encumbered valves in the valve closet. The author did note that a sign has now been placed on the closet door indicating that it is contains the main fire sprinkler valve.

5. Since this was a scheduled furniture reconfiguration, it could have utilized the documented facility drawing recommended earlier, if those documents were in existence. Also, a check of any existing incident-handling plans or disaster recovery plans prior to actually moving the furniture would have been helpful.

6. It is imperative that a "Lessons-learned" session be held after any incident, particularly this one. FCSI has never, in its 12 year history had to deal with an event such as this. However, without the chance to examine what was performed correctly and which areas that could be enhanced, they are ill prepared for future catastrophes.

Conclusions

An incident occurred at FCSI headquarters on a late summer afternoon. Even without proper guidance, documentation and support, the staff sprang into action. They worked to safeguard the technical assets and the most important assets of all: their personnel. Certainly some actions could have been taken to prevent this incident from occurring, and there are obvious areas for improvement, but overall the FCSI staff performed admirably. They should be commended.

Reviewing the six recommendations presented in this practical would go a long way towards better preparing the FCSI staff for future events.

Appendix A - Photographs

Appendix A provides photographs of the damage and the recovery operation at the FCSI NOC.

FCSI employees survey the water on the NOC entryway floor.

Clean up efforts are underway inside the FCSI NOC.

More water damage in the server storage space.