Global Information Assurance Certification Paper

GIAC Advanced Incident Handling and Hacker Exploits

Practical Assignment For FIWC

January 8-12 2001

Option 1 – Illustrate an Incident

A Violation of Trust

(*A threat from within*)

Pamela M. Pirkle

I. EXECUTIVE SUMMARY

What: Our Internet Service Provider reported that our account had been used for greater hours than our records had shown.

When: 14 Jan 01-19 Jan 01

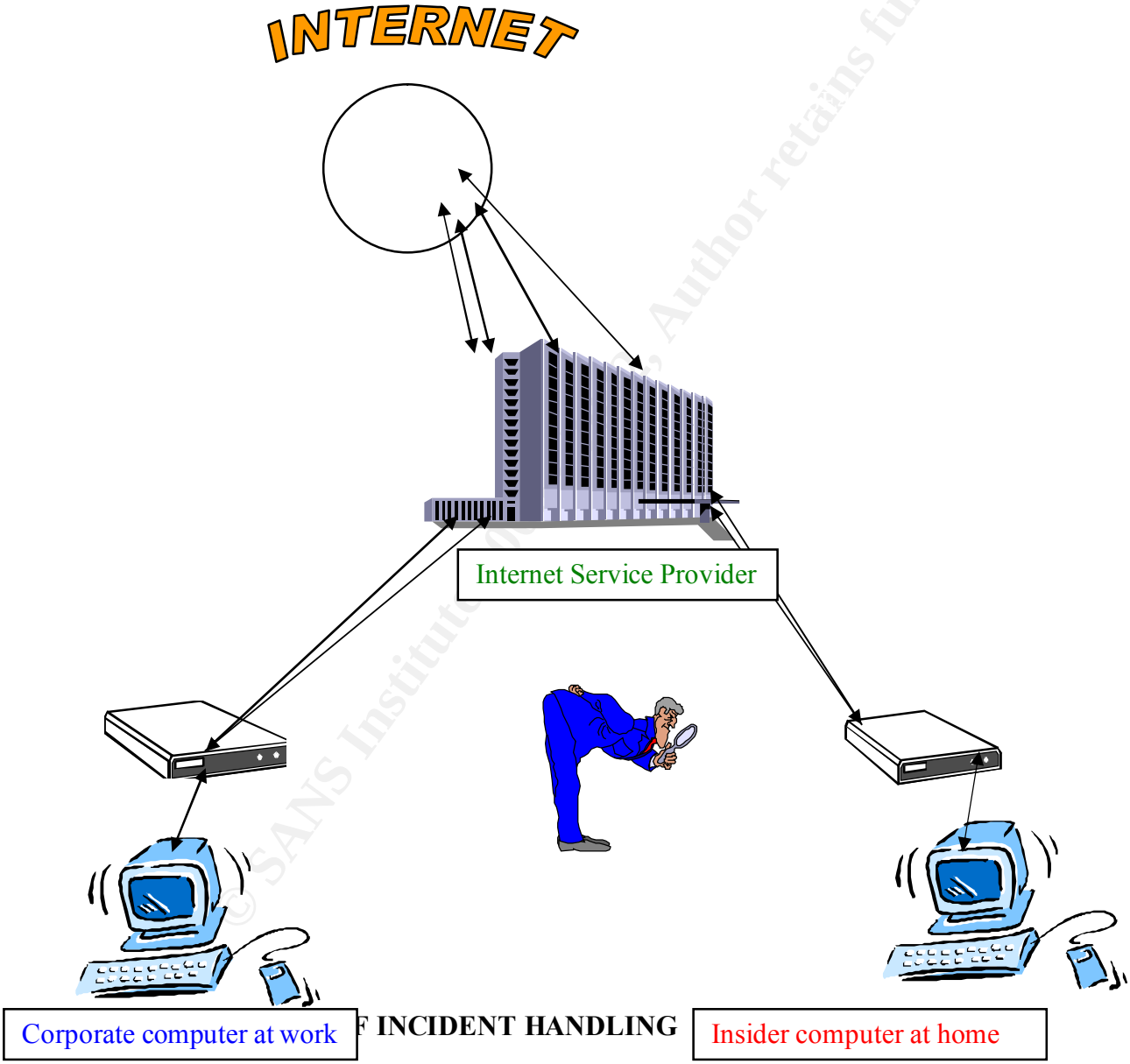
Where: A local address other than the work place

Why: Very smart and curious employee

How: Poor security standards. Gained access using common knowledge

Who: A very trusted employee.

A. DIAGRAM of COMPUTER CONNECTION



F INCIDENT HANDLING

This is a recount of an incident I handled barely one week after attending the Advanced Incident Handling and Hackers Exploits class. Though the attack was not technically complicated and our closely monitored network was not compromised or

even targeted, the investigation revealed issues that left us feeling exposed and vulnerable. A detailed account of the incident at hand follows. This case touched on many issues ranging from fraud, waste, and abuse to how much trust should a company put in one department. When choosing this incident, I asked myself the following questions: "Why do I believe this incident is important enough to base my practical on if there weren't any complicated exploits utilized?" and "How does this pertain to the curriculum discussed in class?" This is what the investigation revealed: the importance of following the six steps of incident handling, knowing the architecture of the Information System to include assets and locations, and the reality that the internal threat is probably the most damaging and disruptive to the business environment.

The details from this incident have been copied from official documentation. Times and dates are accurate. There are six phases to successfully handling an incident and they are as follows:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned/follow up.

These six steps will be in bold for easy identification as the report unfolds.

The incident occurred on Friday, the 19th of January 2001. It was the close of business and like every Information Systems Security Officer I was suffering from the delusion that I might actually escape into the weekend with out incident. At 3:45 p.m., the phone rings. A co-worker had called to report a possible incident. My presence was requested in his office as soon as possible. The initial excitement I felt soon turned into dread as I realized this was my "house" that had been violated. My mind raced with the possible ramifications of a major incident and what I could have done to avoid the situation. Then I realized I was already violating the first thing we learned in class when handling a report of an incident: Remain Calm.
I didn't even know what the chief complaint was. This could be a false positive. So I took a deep breath to relax and focus my thoughts. I then put the first phase into action.

A. PREPARATION

The key to staying calm is having a plan of action. **Preparation:** The first and possibly the most important step. Items that should be considered when preparing an office/ place of business for incident handling are as follows: Policies, People, Transportation, Software/Hardware, Data, Communications, Power, Space, Supplies, and Documentation. Proper preparation helps prevent costly mistakes and protects the integrity of the investigation. One item of interest discussed in class that we had not yet implemented in our office is a Jump Kit. I sincerely believe if this case had been more

complicated, requiring more backups and forensics, the progress this investigation took would have been greatly impeded.

As I was gathering my wits about me and trying to remember all I had learned in the Incident Handling and Hacker Exploits seminar, it dawned on me that I had plenty of experience assisting other place of businesses with handling their incidents. How prepared was my office to handle this properly and smoothly? Some important policies and security guideline were in place for our network, and our hardware and software were up to date with all the latest patches installed. All traffic was monitored entering and leaving the firewall. From an information security aspect we had our bases covered against an external attack. The personnel in our office were well trained in responding to incidences. Plus we had all attended this SANS course, which gave us all more ideas on how we can improve the efficiency in our office. One idea we implemented immediately was the use of a composition notebook to document all actions taken during the investigation. This would prove to be highly valuable at a later date.

So, I grabbed a new composition notebook. Next, I contacted the Security Manager and informed him of the situation. At 4 p.m. we met in the office of the person reporting the incident. We agreed that I would be the person documenting all the steps taken during the investigation. We asked all the questions we felt were pertinent and surmised we definitely had a situation needing further investigation. The complaint was as follows: Our supply office received a phone call from the internet service provider stating that their dial up modem account was 200 hours over the limit and that they would be billed accordingly. The maximum hours per month for this account are 700 hours. The personnel in this office assured us they had in no way accrued so many hours. Their normal usage was under 300 hours per month. This was definitely a flag, and part of the second step in handling this incident. The Security Manager and I would investigate this together.

B. IDENTIFICATION:

Identification is the second phase of the process. Users, system administrators and security officers need to be educated on the following: What signs will indicate an incident has occurred? and, who should be contacted and in which order if an alert is warranted. Alerting others will help minimize damage. Knowing the information system infrastructure throughout the entire company is also very important. The larger the company, the more difficult it is to keep tabs on all the changes people make. Knowing all the above will make it easier to identify if an incident has actually occurred and if there is a benign trigger causing the symptoms. Not being familiar with my office functions could hamper an investigation, possibly leading the investigation off track.

So was the case in this investigation. Remember we (the Security Manager and I) thought we had asked all the pertinent questions. The Security Manager contacted the Internet Service Provider to gather more information. Prior to the call, it was verified that no users were logged into the account from the computer in question. After faxing a company letterhead to the ISP office with our contact information, the ISP verified that

the account was indeed still logged into. Several possibilities came to mind as to what could be causing this. My first thought was that a malicious code or Trojan Horse had somehow been downloaded via the Internet and this dial up system was being exploited. My theory was that this Trojan was resetting the modem, and then dialing out to a preset number. This could have been a more serious incident, because pay records and company expenditures were on this computer. This would not a good thing. To disprove my theory, we disconnected the modem from the telephone jack. The ISP informed us that we were still logged into the account. We knew that we could not be using this account, for the CPU had no connection to the dial up account.

The next theory we discussed was the possibility of someone having sniffed the account over the Internet and had somehow compromised the password. There were more questions for the ISP and the personnel in the office. We determined the password would not have been difficult to crack, because it was a very simple dictionary word. A security hole we did not realize we had. Apparently all users were not as educated in secure communication policies as we had thought. So this was a definite possibility. Since the computer had previously been powered off at the end of each day, and the activity had been occurring the entire month, the CPU was moved to a more secure environment so back ups and forensics could be conducted on the box. At 5:00 p.m. that evening, the person who reported the incident called us to inform us that their dial up account had not been compromised. The person who normally handles the dial up accounts was out of the office for the day. Our point of contact was not aware of any other dial up accounts with in the company. This person believed the account in question was the position they used in their office. It did not occur to me to ask that very important, basic question. What is the name of the account in question? The assumption that this person was familiar with all dial-up accounts at the command cost us several hours. The computer was returned to the office. Case closed? Not by a long shot.

The cooperative Internet Service Provider revealed the login ID and the numbers the account had been accessed from. An inverse lookup on the telephone numbers gave us information that left us stunned. The dial up account had been accessed using our company's information from a private phone line. In retrospect, it was probably the most obvious conclusion. But who wants to believe a person from with in would violate the trust bestowed upon him? Trust is given with what we believe to be an acceptable level of risk. Not much thought is given during day to day operations to the vulnerabilities exposed. But how does one safeguard against this? What techniques were used to exploit this dial up connection? Was an IP spoofed? If the employee pulled this off, what else has this individual attempted or accomplished? How does a company recover from this? But before we could deal with these issues completely, we had to enter into the third step in the incident handling process.

C. CONTAINMENT

Containment is the process of isolating the incident to the areas known to be affected, so as to avoid the spread of the incident. We don't want the problem to get worse. In the case of a root compromise, or malicious code, removing the system from

the network is the first step. A system that has had a root compromise would need to be backed up so as to keep the integrity of the evidence with in the log files. But how do we contain such an incident? We were not sure the extent of the damage to our company. There was one thing we could do with the cooperation of the Internet Service Provider (ISP) with these facts in mind. We contacted the ISP again and asked their agent for a copy of the log files. We would not be able to obtain these until Monday. Until then we needed to stop the exploitation of this account. This account was essential to our operations. Research revealed the account should have been billed as unlimited. A clerical error had created an account limiting usage to 700 hours account. Had the account been properly tagged, the incident would not have been revealed. This fraud could have gone on for years. Just how long had it been occurring? We might never find this out. The main thing we needed to do at this point would be to deny the perpetrator access to the account.

Again we worked with the ISP representative. We informed him that this account should be unlimited billing and we asked what could be done to reflect this change without interrupting our operations. This account was necessary to the operations and would require extended usage. The provider determined that adding an identifying character to the front of the login in name would effectively update the account. We would have to change our login and password on our end. Since the individual was unaware of this change, he would effectively be denied access to the account. With the emergency of the situation contained, more questions loomed. What could keep this from reoccurring? Could the person regain access through the same means? How did he gain access? Did he spoof the IP from home? Is this a common practice in his department? Did this person act on his own will? With more questions than answers, we swiftly entered into the next phase of this operation.

D. ERADICATION

Eradication is the most difficult phase of the incident handling process. Using the information gathered during the previous phases, the incident handler needs to isolate the attack and determine how it was executed. Careful scrutiny of any files once a back up has been made should reveal what exploit was used. Sometimes it could be obvious such as a malicious code. Other exploits could be more difficult to find. Good training and practical experience help with these procedures. Once the cause of the incident has been revealed, action needs to be taken to prevent it from reoccurring. Improved defenses such as firewalls, anti-virus gateways, moving the system to a new IP address are a few ways to accomplish this. The cause of the incident must be removed. The most recent clean backup should be used. Patches for the vulnerability must be in place. If the exploit isn't fixed, the system is still vulnerable.

So how do we uproot this internal threat? By using the information we gathered in the previous phases, we were able to determine that the computer in our office spaces had not been compromised, but that the IP had been utilized from another phone line. In essence, someone had stolen/ borrowed our dial up account information. This would

equate to crafting a packet in a TCP connection and spoofing the IP from another network.

Copies of log files obtained from the ISP revealed that the phone number used was not from our place of business and resolved to an employee's private number. These files also revealed that the login attempts were not automated. There was not a rhythm to successful and failed logon attempts. Once access was gained, the amount of time logged into the account varied from as short as 3 seconds to as long as 1 hour. The ISP was very cooperative through out the investigation and compiled a hard copy of the files to assist us with the investigation. A sample excerpt from the logs appears as follows: XXX indicates the private phone line and 000 represents our office number.

Jan 14 17:56:27 Jan 14: 17:56:39 Shark4, S9 0d 00:00:12
28800 28800 (XXX)XXX-XXXX Admin-Reset
LAPM/V42BIS LAPM/V42BIS

Jan 14 17:57:52 Jan 14 17:58:06 Shark4, S9 0d 00:00:14
49333 49333 (000)000-0000 Admin-Reset
LAPM/V42BIS LAPM/V42BIS

In this instance, both computers are attempting to login at the same time and the ISP systems sends an admin reset to drop the connection. The logon attempts from the private number are intermittent and did not appear to be scripted.

Jan 15 18:24:14 Jan 15 19:48:00 Shark6, S27 Od 01:23:46
26400 26400 (XXX)XXX-XXXX User Request
LAPM/V42BIS LAPM/V42BIS

The longest period of time the private number was log into the account was 1:23:46. This occurred after normal working hours from 18:24:14 – 19:48:00 . The log off request for this instance was identified as user-request.

What was this person doing during this time? Was any thing malicious occurring? These questions were researched and it was determined that no malicious activity had been initiated from these logons in the name of our company. We still needed to determine two things: How this person gained access to the account information, and how was the account accessed from home.

It was determined that this dial-up account was utilized in this person's office for special projects. Everybody in this office space had access to this information. All personnel with in these spaces were computer competent and would know how to create an account. The login name and password were common information with in this department. Access was not limited to a few people.

With the information gathered, it was determined to deny the employee in question access to the spaces for the duration of the investigation. Rights were read and questions asked. This person admitted to spoofing the account information from home. It was just a matter of having all the information and setting the home computer system up to match the account from work. The only glitches that hindered the operation were when the two computers (from home and work) would attempt to access the account at the same time, which explains the admin resets previously displayed, and the ISP inquiring into the over usage of hours.

To completely eradicate this vulnerability from our spaces would be great! The easiest thing would be to prosecute the perpetrator and that would remove the threat. Or so one would hope. Our company trusts hundreds of people with very sensitive information. Remember, if this account had been billed properly, the fraud, waste, and abuse of company assets would never have been identified. So this vulnerability would prove to be more difficult to remove.

The following steps were taken to minimize our risks.

1. The employee was denied access to the workspaces while the investigation concluded.
2. The account was changed to deny this person access from home.
3. Random review of account logs to ensure our assets are not being exploited. Review would include hours accessed and telephone numbers.
4. Audits and vulnerability analysis to help us monitor activity on dial up accounts and their designated workstations.
5. Tracking/logging software should also be installed on these systems.

I feel the most important step that can be taken to prevent such an event from happening again is education. We all need to be aware of our work environment. Know your Information Systems. Know your people and Personalities. Are people working odd hours? Is any one being more inquisitive than would be expected? How many dial-up accounts do we actually have? Are people trained on the security aspects? Is there a user agreement outlining expected and prohibited behavior? People should never be afraid to always question unsettling behavior.

With these important factors noted: who, what, when, where and how this incident occurred and the reasonable chance at removing the threat we moved into the recovery phase.

E. RECOVERY

The fifth phase of incident handling is **Recovery**. To properly accomplish this the following steps should be followed.

1. Restore from backups: Every effort should be made to ensure compromised code is not being restored.
2. Validate of system: tool. Once the system has been cleaned up, it must be validated. Tripwire could be a helpful tool
3. The system must be operational and baseline documentation should be generated.
4. Finally, operations must be restored. The decision to restore operations should be put in the hands of the system owners.

In this case, recovery was not so simple. Yes, our operations were still in tact. No back ups were necessary, because our computer's operating system was never compromised. What had been exploited was at the core of our day to day operations: Trust.

The company's trust in its personnel had been violated. Though some believed a few stolen hours of Internet time wasn't much to be upset about, I saw a much greater vulnerability. We are as weak as our greatest acceptable risk. I believe our weakest link to be the insider threat. Safeguards can be put on hardware, sensors, firewalls and internal monitoring. But there is no way to control what a person walks away with in their minds. Access can be controlled to a certain extent by determining need to know and compartmentalization of information. But we still need a way of determining who will exploit the information to which they are exposed.

Recovery for us consisted of:

1. Firing the employee.
2. Disseminating information throughout the firm on how important it is to guard against the internal threat.
3. The dangers of Social Engineering were highlighted and briefed to all personnel.
4. All dial-up accounts are now monitored for anomalous activity. Random checks are important.
5. User awareness has been generated via User agreement contracts when accounts are assigned to employees.

Educating the employees on the danger of social engineering is a must. Social engineering can be conducted from within and is not always an external threat. Employees who are too inquisitive about issues that do not pertain to their job, or keep odd hours should be noted. The operant in our case had been classified as a highly inquisitive person and highly regarded for professional knowledge and all around nice person. Those assumptions gave us a fine example of how social engineering can create leeway for a person to conduct harmful activity against their place of business.

Anther step in our recovery phase was to demonstrate to all personnel that this behavior was unacceptable and will not be tolerated. The accused in this case was charged with fraud, waste and abuse of company resources. An executive hearing was conducted and appropriate disciplinary action determined. To this point, all the evidence we had

gathered had been documented in my composition notebook and put into a case folder. The case folder contained the following: an original hard copy of the log files obtained from the ISP representative, a time line of events and actions taken as documented in the composition notebook, and a summary of the hours the accused had accrued while logged into the dial up account.
This evidence was crucial during the prosecution.

Now that the recovery phase had been completed, we needed to document all that we had learned during this endeavor. An after action meeting was called. This moved us into the final phase of incident handling: Lessons Learned.

F. LESSONS LEARNED/AFTER ACTION

The process of documenting all the lessons learned and filing the after action reports during the handling of an incident is the last phase in the six steps to incident handling. We held an after action meeting with the team members who handled the incident. Two lists were drafted: "Security Issues " and "Process Improvement". The first list titled "Security Issues" details steps to be taken to minimize the threat to our work environment. The second list named "Process Improvement" provides feedback on how we handled the incident.

I. Security Issues

1. Security Manager and assistants need to be more aware of the entire IT infrastructure. This incident went beyond the Internet. Dial up accounts existed that we did not know about.
2. An up to date inventory of each departments assets needs to be generated and supplied to the security office.
3. All departments should be randomly audited for compliance to policy.
4. An individual in a work center given too much freedom could be tempted to exploit a practice unsafe to security.
5. We needed to educate people on the importance of knowing their office environment. Who is working on which project? What working hours are being kept? What equipment belongs to their office? Who has Internet access?
6. We need to stress that social engineering and the insider threat is actually very common.
7. As the security office we shouldn't assume that our own house is clean.
8. Though the external threat is important, more attention needs to be given to preventing the internal threat.

II. Process Improvement

1. Documentation:

A. Proved to be very important in the prosecution of this case. The detailed report was crucial in validating the integrity of the investigation.
B. Copies of all files need to be retained for future reference. Once this case was turned over to the prosecutors, our case file was requested as evidence. Copies were not retained for our files.
We need to update our policy to reflect this suggestion.
C. Times and phone logs. Not all conversations and phone calls were documented as they occurred. We need to ensure all log entries include the date and time.

2. Preparation:

A. We should have a jump kit available for all handlers

B. Create a set of procedures for handling all types of incidents. Our primary focus had always been guarding against the external threat. Procedures need to be developed to include actions necessary when dealing with the internal threat.

C. Treat all incidents as though they are serious. Something simple could prove to be a serious infraction to security.

D. Create policy and user agreements limiting dial up access. Ensure penalty for violation is stated.

3. Identification:

A. Do not jump to conclusions. Ensure all facts are gathered and are correct. Remember when identifying an incident take all evidence into account.

B. Ensure the person you are working with has accurate knowledge of their spaces and personnel.

C. Don't assume nice guys won't break the law. This assumption set us back a few hours in the investigation.

4. Containment:

A. When assessing risk, damage to the company may not be just monetary value. The cost for over hour usage was only $200.00. The cost associated with the investigation weighted with the loss of a trusted employee and/or information that may have been exploited makes assuming the risk more dangerous.

B. We failed to make a copy of the computers hard drive prior to powering it down. Though this particular computer proved not to be the victim, we could have destroyed valuable evidence. If the evidence had not been destroyed, the integrity could have been questioned by the defense.

3. Eradication:

   A. Tighter control over company assets needs to be maintained.

   B. Although we did not need to restore any information, it was discovered that the office in question did not have back-up copies for some of its software. A central storage for all software utilized by the company would alleviate this issue.

4. Recovery:

   A. Communication was restored immediately to the computer we originally suspected of compromise once the office manager was assured they were not at risk. Prior to restoration, we required the passwords be upgraded to comply with company policy.

   B. We need to streamline and document a chain of command for decision making concerning access to accounts. It took four hours from report of incident to the recovery phase to get the dial up account logon ID changed. The supervisors of the individual enacting the event wanted to cover for their personnel stating that the activity might have been authorized. A lot of damage could have occurred in this time frame.

III. CONTAINMENT PROCESS

As stated in the containment phase of this report, resolution was as simple as changing the logon ID for this account. The Internet Service Provider identified there was a problem when the account billing was over hours. Once the Security Manager was notified, a more detailed look into the account ensued. The ISP was contacted via telephone. All troubleshooting occurred via the telephone.
The following occurred:

1. ISP technician (Tech) was able to query the log files for all the activity generated from our account. He used an automated menu to accomplish this.

2. All telephone numbers listed in the logs were revealed to us during this phone conversation. We did not recognize one of the numbers listed.

3. Technician revealed their operating system is Unix based

4. We determined the telephone number was local to our area

5. Tech performed an inverse look up on the number and was able to reveal the name and address of the person currently logged into the account. He did not state what search engine he utilized.

6. We queried our NT database of personnel and identified the person as our employee.

7. As stated earlier, we did not have a jump kit on hand. The technician from the ISP did not reveal if they had a jump kit to assist them with their trouble calls.

8. He did reveal it is their standard procedure to notify the consumer if there are any strange occurrences.

IV. BACK-UP PROCESS

1. Due to the nature of this incident, we did not need to back up our computer.

2. The ISP performs back ups on a weekly basis. They would not reveal what techniques they use.

V. CHAIN OF CUSTODY

1. All activity was logged in a composition notebook.
2. Date and time of all actions logged along with all findings as each step of the investigation ensued.
3. Law enforcement was notified. Forensics was not necessary for our local computer. Because root access was not obtained, it was determined the activity log files from the ISP would be enough evidence to prosecute.
4. Once the log files were obtained from ISP, they were included in the case file.
5. All evidence was kept locked up with access granted to the Security Manager and the investigating officer.
6. A confession was obtained from the accused. The confession was subsequently included in the case file.
7. At the conclusion of our investigation, all evidence was turned over to the prosecution.
8. The prosecution has maintained custody of all evidence.

9. Successful prosecution resulted from the following evidence
   A. Log files with the telephone number of the accused
   B. Resolution of the telephone number to the address of the accused
   C. A signed confession from the accused.

VI. MORE INFORMATION ON NON TECHNICAL INSIDER THREAT

The insider vulnerability has plagued our most prestigious government agencies. Recently, the Federal Bureau of Investigation arrested one of their own people and charged him with espionage. The complete story can be found at this link: http://www.msnbc.com/news/533071.asp

Mr. Hanssen had been employed by the Bureau for fifteen years and was a skilled programmer. Concern existed that the accused could have created vulnerabilities with in government computer systems that would allow spies to steal sensitive information. The March 5th article reveals "The government alleged that since 1985, Hanssen passed to Soviet and later Russian contacts 6,000 pages of top-secret documents containing information about how the United States conducts intelligence operations, which foreign agents it has targeted, and technical data about communications and surveillance."[1] The extent of the damage caused by this alleged insider's actions has yet to be fully revealed. This story proves how vital it is to protect our work environment. No person is above question. The most trusted person is capable of causing the most critical damage.

Bob Cohen reiterates the seriousness of the insider threat in an article I found in Infosec Outlook May 2000 Volume 1, Issue 2 A joint monthly publication of the Information Technology Association of America (ITAA) www. itaa. org and the CERT® Coordination Center (CERT/ CC) www. cert. Org. In his article *Hacked off... The Experts Call Hacker Motivation Key to Prevention,* Bob Cohen quotes Paul E. Proctor, author of *The Practical Intrusion Detection Handbook*, released in July 2000 by Prentice Hall. Proctor states that "Eighty-five to ninety percent of losses are insider incurred." He calls "external hackers a growing annoyance but not necessarily growing threat." [2] As a whole, we need to take a closer look at the risks looming in every work center, and be proactive with our security efforts to contain the threat within.

The entire article is located at the following URL: http://www.cert.org/infosec-outlook/infosec_1-2.pdf

VII. MORE INFORMATION ON SPOOFING

[1] NBC News producers Jim Popkin and Robert Windrem and The Associated Press contributed to this[1] report. MSNBC STAFF AND WIRE REPORTS

[2] The Practical Intrusion Detection Handbook, released in July 2000 by Prentice Hall

Although the IP address was not spoofed in this incident, all the account logon information was. Depending on the attacker's goals and motives, he could have achieved the same results using an IP from our network. The individual did have access to all this information.

1. For more information of spoofing techniques and exploits please refer to the following:

http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=spoofing

www.cert.org/advisories/CA-95.01.IP.spoofing.html

VIII. REFERENCES

[1] NBC News producers Jim Popkin and Robert Windrem and The Associated Press contributed to this report. MSNBC STAFF AND WIRE REPORTS

[2] The Practical Intrusion Detection Handbook, released in July 2000 by Prentice Hall

http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=spoofing

www.cert.org/advisories/CA-95.01.IP.spoofing.html

Last Updated: May 28th, 2017

Upcoming Training

SANS Madrid 2017	Madrid, Spain	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Virginia Beach SEC504*	Virginia Beach, VA	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017 - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
Mentor Session - SEC504	Reston, VA	Jun 13, 2017 - Aug 01, 2017	Mentor
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Seattle SEC504	Seattle, WA	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS ICS & Energy-Houston 2017	Houston, TX	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Ottawa SEC504	Ottawa, ON	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Sacramento SEC504	Sacramento, CA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Annapolis SEC504	Annapolis, MD	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Phoenix SEC504	Phoenix, AZ	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Des Moines SEC504	Des Moines, IA	Jul 24, 2017 - Jul 29, 2017	Community SANS
Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
Community SANS Raleigh SEC504	Raleigh, NC	Aug 07, 2017 - Aug 12, 2017	Community SANS
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event