Global Information Assurance Certification Paper

COMPUTER SYSTEM INVESTIGATIONS

Russell R. Densmore

GIAC Security Essentials
Certification (GSEC)

Practical Assignment

Option 1

SANS Institute

October, 2004

TABLE OF CONTENTS

Russell Densmore

ABSTRACT

With the proliferation of computing systems in today's society, the robustness of the security of those systems is coming to the forefront of public opinion. The reason for this is due to the lack of security that should have been implemented when the computing systems were built. However, it is very important to understand and investigate the security breaches of computing systems. By investigating those breaches we learn from those incidents to prevent similar future security problems.

We all know that computer system security breaches do occur[1], and are increasing[2]. The computer system investigator chooses to look for this type of abuse of computing resources, and prepares the case report to take action against those perpetrators[3].

[1] "Hacker hits California-Berkeley computer: Attack accesses 1.4 million Californians' Social Security numbers." CNN.com

[2] Susan W. Brenner, *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships.*

[3] Carole Fennelly, *On Trial: Prosecuting cybercrime puts your organization—and your security—on the hot seat.*

Russell Densmore

THE NEED FOR COMPUTER SYSTEM INVESTIGATIONS

In today's society, information is moving faster and faster. From corporate networks, to cell phones, and gaming systems, the spread of computer systems is growing rapidly. It seems that every where we look, information systems are spreading at a daunting pace. Often times, these systems are developed with "time to market" as a key driving factor, dismissing the need for proper security requirements. This philosophy has helped the rapid expansion of technology, but has left major problems to be cleaned up on the back side. The development of these systems with only minimal consideration given to security features, have allowed "hackers" to proliferate. Therefore, the ability to detect information compromises and the ability to remediate information system abuse has grown. Hence, the needs to effectively investigate, prosecute, and learn from these security breaches has grown.

Many corporations find themselves needing to collaborate amongst employees, departments, divisions, outside contractors, and to support satellite locations. The need to have tools that can be utilized over broad areas, and even across continents drives corporations to utilize or develop tools that make it easier for these components to share their work.

Making communications easier for business usually dictates using items that have functionality in mind, not security. Yet these same corporations may be devastated by the loss of their intellectual property, or the intellectual data that gives them a competitive advantage. The communication and collaboration tools that are implemented must then be both business enabling, and also secure. These two positions may appear to be difficult to accomplish. However, with the proper training and security elements incorporated into the entire life cycle of the program, both security and functionality goals can be met.

What happens when the security of these systems does not meet its stated objective, and the system is compromised, and potentially harmful information has fallen into the wrong hands? In 2000, the FBI discovered that they had a spy by the name of Robert

Hanssen[4] who was using computer systems to encrypt and hide information as well as use wireless computing devices to communicate. The following was taken from one of the floppy disks released from their investigation:

> *"As you implied and I have said, we do need a better form of secure communication…faster. In this vein, I propose (without being attached to it) the following: One of the commercial products currently available is the Palm VII organizer, I have a Palm III, which is actually a fairly capable computer. The VII version comes with wireless internet capability built in. It can allow the rapid transmission of encrypted messages, which if used on an infrequent basis, could be quite effective in preventing confusions if the existence [sic] of the accounts could be appropriately hidden as well as the existence [sic] of the devices themselves. Such a device might even serve for rapid transmittal of substantial material in digital form. (US vs. Hanssen)"*

Digital information can be both valuable, and destructive (especially in the wrong hands). This is where hackers come into play. They desire to obtain information or services that they do not have the legal right to obtain. Some do it for personal reasons. Others do it with malicious intent[5]. Whatever the hacker's intent is, it does not change the need for individuals and corporations to protect their information from falling into the wrong hands.

WHAT IS COMPUTER SYSTEM INVESTIGATIONS?

Computer system investigation is a major contributor to any information security program. The investigation of computer system breaches and misuse provides for Root Cause Analysis

[4] United States of America vs. Robert Philip Hanssen

[5] Dave Pettinari, *Investigating Cyber Crime/Hacking and Intrusions.* Pueblo High-Tech Crimes Unit.

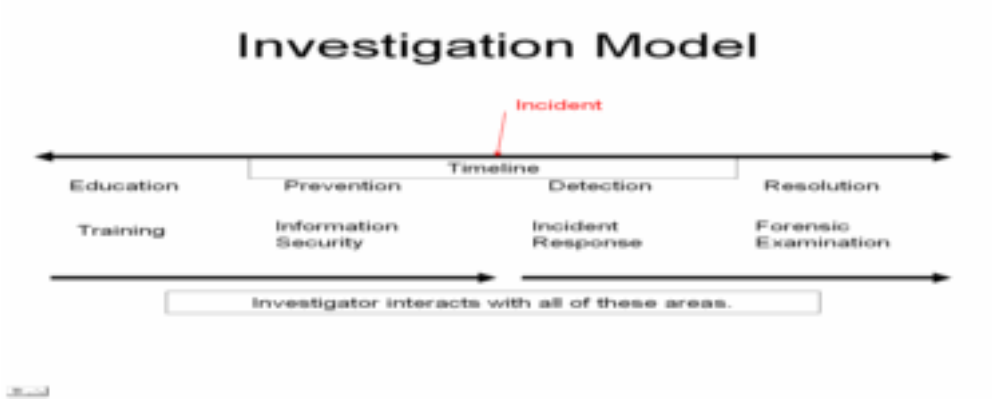
(RCA), Multi-linear Events Sequence analysis (MES)[6], and lessons learned. These provide useful information for resolution and remediation. They also create the basis for education and prevention of future occurrences.

Computer system investigators must understand that their main goal is to oversee the entire investigation process. This would include using normal investigative procedures for the collection of evidence, the handling of suspects, and reporting of their findings. The investigator should apply standard operating procedures to every case. This will allow for consistent and reliable investigations.

THE INVESTIGATION MODEL TIMELINE

There are four major categories of the Investigation Model Timeline (see figure 1)[7]. Those categories are education, prevention, detection, and resolution. These four categories represent the life cycle of information security awareness. A computer system investigator should directly affect all of these areas with the work performed. The beginning of an investigation often occurs at the detection stage (Computer incident)[8], but should continue throughout the resolution, education, and prevention stages to maximize effectiveness.

Figure1



[6] Ludwig Benner Jr., *Investigating Investigation Methodologies.*

[7] Kevin Kearney, *Key Objectives Presentation.* June 24, 2004

[8] Douglas Schweitzer, *incident Response.*

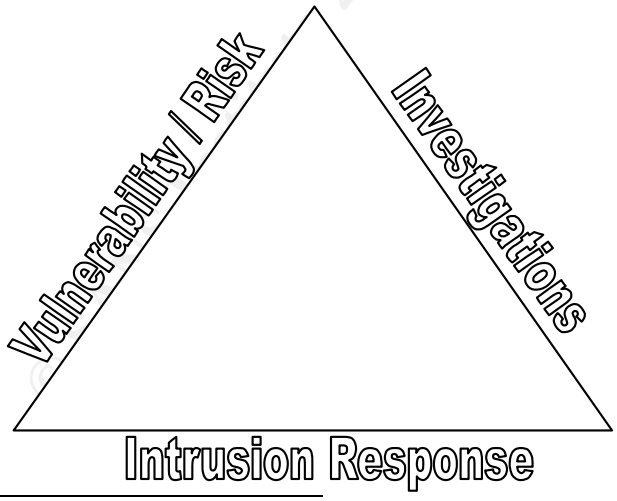
Many corporations use specialized subject matter experts to perform their corporate investigations, however, it has been shown that it is in a company's best interest to keep the investigators, examiners, trainers, and incident handlers separate and focused on their individual tasks[9]. This allows each group to remain focused on their primary objectives, and to not become entangled in the entire investigative process. Thus resources remain focused and engaged.

INFORMATION SECURITY TRIAD

Security professionals need to work as a team to make sure that their computer environment is secure. Computer System Investigations is only one part of the three sides of the Information Security Triad[10]. The network information security environment triad would include the following parts:

- Vulnerability Assessment Team & Risk Management Team
- Intrusion Detection System & Incident Response Team
- Computer System Investigations

Figure 2



[9] Lee Youngflesh, Senior Forensic Consultant, Guidance Software. *Developing a Forensic Response Unit*. Webinar hosted on August 12, 2004.

[10] Bill Nelson*, Computer Forensics and Investigations.*

Each of these groups or departments have different functions and procedures, however, they should assist each other when it comes to conducting computer system investigations. Each group has independent strengths and weaknesses that can provide valuable information in the course of an investigation.

The Vulnerability Assessment Team and Risk Management Teams are responsible for the integrity of the network servers and stand alone computers. They check for weaknesses in the operating systems and applications. They often launch controlled attacks against the network to determine vulnerabilities that may be present.

The Intrusion Detection and Incident Response Teams are responsible for monitoring intrusions, intrusion attempts, and attacks from external sources. If an intruder actually attacks the network and causes significant or possible damage, the Incident Response Team will quickly move to minimize any damage the attacker may cause. They will also be instrumental in the collecting and preserving of evidence that may be used in civil or criminal prosecution.

The Computer System Investigations group is responsible for the management of cases and, conducting forensic analysis of computers used in the commission of a computing event. The investigation group should draw from all available resources to complete a thorough case review. They should ensure that evidence is properly collected, and handled. They will also prepare the reports required to deliver the investigation to the proper authorities for civil, criminal, or administrative action.

ELEMENTS OF INVESTIGATION

There are several elements that are used in most every case of computer system investigations[11]. They are listed as:

- Data Collection
- Digital Evidence Controls
- Forensic Analysis
- Recovering Images
- Investigation Reports

DATA COLLECTION

The beginning of an investigation process is very important to the outcome of the case. Improper handling may render portions, if not all of a case worthless. The proper handling of digital evidence is critical to a successful outcome. The rights of suspects must also be taken into consideration. It is imperative that all evidence collection and handling of individuals complies with state and Federal laws so as to maintain the validity of the information to be used in civil, criminal, or administrative proceedings[12].

PRESERVATION OF "ORIGINAL EVIDENCE"

Original evidence refers to the actual digital medium that contains the data in question. It is very important that the original evidence is not altered in any way. The exact handling of all the different types of media is beyond the scope of this paper and will not be addressed here. However, it is important to note that handling of hard disk drives, floppies, and CD's each present different challenges to ensure that the evidence has not been altered. As an

[11] Bill Nelson, *Computer Forensics and Investigations.*

[12] John Patzakis Esq., "*Electronic Evidence Discovery: From high-end litigation tactic to standard practice.*

example, it would be impossible to write (change) any information contained on a CD without placing it into a CD writer. Conversely, if you attach a hard drive to a computer, and do not ensure the proper write blocking tools are used, you will immediately alter the hard drive upon mounting the disk. This type of action could render the digital evidence unusable.

DIGITAL EVIDENCE CONTROLS

All digital evidence that is gathered should be treated as though it would be used in a criminal proceeding. This would include properly securing the evidence at a scene, as well as processing, handling, and keeping "chain-of-custody" for the evidence[13]. Storage and retention of data must also be addressed. The proper way to prove that the digital information has not changed is to use a digital signature (known as a hash value) on the evidence. Currently the MD5 and the SHA1 hash have been accepted in many courtrooms as a proper method to prove the data has not been altered[14].

FORENSIC ANALYSIS

The procedure used for forensic analysis of digital media may change based on the nature of the type of investigation. As an example; a criminal case involving a specific charge of embezzlement, may be restricted by the court order to only seize the evidence that is related to the embezzlement charge. Whereas, a civil process that is being conducted for a corporation may be wide-spread in scope, and the attorneys may request all information available on the computer be obtained. Be sure that you are aware of the laws that govern the forensic analysis that you are involved in.

The forensic analysis of computer systems may also be directed by the type of investigation being completed. A misuse of a Computer system for the personal enjoyment of viewing pornographic images will be a quite different investigation than an investigation into harassment via email. The computer environment and the

[13] *How the FBI Investigates Computer Crime.*

[14] John Patzakis, *EnCase Legal Journal: Second Edition.*

processing abilities are changing daily. A good investigator will know how to ask for assistance from the proper individuals responsible for the computer system during their investigation. Network administrators, firewall administrators, and others can yield valuable forensic information about what has occurred on a network. Know when to engage them, what information you can share with them, and what not to share with them. Above all, make sure that you give them credit for their work.

RECOVERING IMAGES

Remember the phrase "A picture is worth a thousand words?" That is true for computer system investigations. Many times, an image recovered off of a suspect hard drive can change the direction of an investigation. None is truer than when images of child pornography are found. If child pornography is discovered during forensic examination, legal counsel, and criminal authorities should be notified. There are strict laws about the reporting of crimes against children. A forensic examiner should not continue to examine a computer system where child pornography exists. Continuing the investigation and review of child pornography places the investigator at risk. Your legal counsel should be notified immediately.

IMAGE FILE FORMATS

There are many types of image file formats that most graphic editors will allow someone to save image files as. The most common formats include Joint Photograph Experts Group (.jpg or .jpeg), Graphics Interchange Format (.gif), Tagged Image File Format (.tif or .tiff), and Windows Bitmap (.bmp). There are several other less common image file formats[15].

It is important to understand that analysis of computer systems cannot rely solely upon the file extensions as mentioned with the image file formats. An image could easily have the file extension changed to reflect another type of file. In these cases, it would be important for the investigator to have a proper tool that will allow for the comparison of the file header information to the file extension.

[15] Website: http://www.library.cornell.edu/preservation/tutorial/presentation/table7-1.html

This would reveal any files that have an extension that does not match their file header. These files would be very suspicious, and should be reviewed as part of the case. Several forensic tools on the market provide for this type of analysis.

INVESTIGATION REPORTS

The most important part of any Computer system investigation is the reporting of the information discovered. The relaying of critical details, or the lack thereof, is what provides law enforcement, legal counsel, or administrative personnel the ability to take action. The proper dissemination of the facts discovered is what may compel a response or not.

The reporting of information from the investigator should be limited to reporting specifics. The report is not where any assumptions, recommendations, or personal feelings belong. The investigator should write the report using the 3 C's.

- Clear
- Concise
- Correct

A clear design and layout of a report will make it easier for the investigator to report the facts uncovered[16]. A consistent format for reporting is advised. This will allow your readers to understand the findings presented to them more quickly as they become familiar with your reports.

The investigator must right clearly, and "say what you mean, and mean what you say." This simply means that you do not write vague statements. As an example; it is not sufficient to say that you discovered image "*x*" on the suspect hard drive. It is much clearer, and meaningful to state "On June 12, 2004, this investigator performed forensic analysis on suspect Jane Doe's

[16] Bill Nelson, *Computer Forensics and Investigations.*

seized hard drive (evidence item 4). The forensic analysis was accomplished using *Forensic Toolkit* by Access Data. The forensic software is a licensed copy. At about 16:30 hours GMT, I discovered "image x", which is related to this case.

Notice that there are no conclusions drawn about the image, nor what anyone else should assume. Let the reader review the evidence item, and make a determination about the evidence provided. Provide factual information about who, what, when, where, and why.

CONCLUSION

Performing computer system investigations is a complex and delicate process. There are several issues to deal with, and several methods to follow. Improper handling of digital media can ruin an investigation, and even make the investigator held civilly or criminally liable for their actions. Therefore, it is imperative that the investigators are properly trained and prepared to fulfill their duties. Proper handling of the investigation will assist with a successful outcome.

Proper training and practice is an important first step for any computer system investigator. The training should involve investigation procedures, data acquisition, forensic analysis, report writing, and communication skills. A solid grasp of all of these areas will be needed to effectively communicate the results to management, attorneys, law enforcement, and potentially to a judge and jury. Every step of the investigation process may come under scrutiny, and only a trained professional that consistently performs the investigations under the same strict protocols and procedures will be able to stand firmly behind their work.

LIST OF REFERENCES

Nelson, Bill, Amelia Philips, Frank Enfinger, and Chris Steuart. Computer Forensics and Investigations. Boston: Thomson, 2004.

Schweitzer, Douglas. Incident Response: Computer Forensics Toolkit. Indianapolis: Wiley, 2003.

Middleton, Bruce. Cyber Crime Investigator's Field Guide. Boca Raton: Auerbach, 2002.

Investigations Guide. Bethesda: Lockheed Martin Corporation, 2004.

Fennelly, Carole. "On Trial: Prosecuting cybercrime puts your organization--and your security—on the hot seat." Information Security Magazine October 2004. <http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss486_art1001,00.html.>

"Hacker hits California-Berkeley computer: Attack accesses 1.4 million Californians' Social Security numbers." CNN.com 20 October 2004. 29 October 2004 <http://www.cnn.com/2004/TECH/internet/10/20/crime.hacking.reut/.>

"Oxford suspends two Students over Hacking." News.Scotsman.com 29 October 2004. 29 October 2004 <http://news.scotsman.com/latest.cfm?id=369104.>

"How the FBI Investigates Computer Crime." CERT Coordination Center 27 July 2000. 24 October 2004. <http://www.cert.org/tech_tips/FBI_investigates_crime.html>

Website: <http://www.library.cornell.edu/preservation/tutorial/presentation/table7-1.html>

Brenner, Susan W. "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships." North Carolina Journal of Law and Technology Volume: 4 Issue: 1 Fall 2002.
Pettinari, Dave. "Investigating Cyber Crime/Hacking and Intrusions." Standard Operating Procedure: Pueblo High-Tech Crimes Unit 1 April 2000.

Patzakis, John M. "Electronic evidence discovery: From high-end litigation tactic to standard practice. Federal Discovery News. September 2000.

Patzakis, John M. "EnCase Legal Journal: Second Edition" March 2002.

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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 San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
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
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
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 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