Global Information Assurance Certification Paper

Criminal Forensic Investigations

Use of Supportive Presentation Tools

In a Successful Investigation

By William Burns
GSEC Practical v. 1.4b, Option 1
May 4, 2004

Abstract

Successful internal company investigations are greatly assisted by carefully crafted presentation tools used to gain managements' understanding and support, while providing the basics of what happened during the investigation. The importance of, and value added when using presentation tools to support internal investigations of employee wrongdoing is significant. They provide company management a clear, concise picture of what was found out. Carefully crafted presentation tools set the stage for decisive decision-making regarding the matter under investigation.

Supporting Tools:

- Investigative flowchart depicting the people, personal businesses, clients, vendors, and third party consultants used by the suspects
- Word document showing generic opening and closing statements used for the interview process
- Spreadsheet detailing the review of the seven suspects' Email, telephone, VPN, instant messaging and non-business computer usage
- Final Report Template used to document the case
- Forensic Hardware and Software Tools

Background

On MMDDYYYY, a caller (name refused) to the Ethics hotline stated he/she heard from another individual that a Company employee (Prime Suspect) was conducting a personal business on company time, using company resources and associates (names unknown). The claim was based on a conversation among staff, overheard in the company cafeteria during lunchtime. The caller stated the business is a computer consulting business that does network installations and monitoring. The caller was instructed to call back on MMDDYYYY, but never did. The matter was referred to Investigation Services to investigate.

The initial scope was to review the Prime Suspect's Emails and information residing on his/her personal computer(s) and determine if the allegation merited further investigation.

Investigation

- **Initial Steps – Week 1**

Access privileges to the Prime Suspect's email and Personal Computer were obtained for the length of the investigation[1]. This access was then used to covertly review information remotely.

[1] The author recommends that this type of access be obtained on a permanent basis but the password be kept in secure manner (i.e. a safe) until needed. and the password changed when the investigation is completed. In this way access is available only when needed and the potential for deliberate or accidental abuse is limited.

The entire mailbox was copied and stored in a separate vanilla folder[2] and then copied to a working folder on a separate hard drive. Only the data in the working folder would be accessed during the investigation. This was done to ensure that originals would not be compromised. This methodology would be maintained throughout the investigation. The entire mailbox and logical hard drive data were remotely copied and saved in these same folders.

- **Investigative Analysis – Week 2**

  The Email and PC review of the Prime Suspect disclosed that the allegation appeared true. Six other Company employees were found to be involved in supporting the Prime Suspect's personal business(es). We found that the Prime Suspect used different personal business names in dealing with a number of clients. In addition to Company employees, a number of vendors and 3rd-party consultants were being used in supporting these clients.

  The email review showed that the Prime Suspect appeared to have nonstandard business relationships with at least one person at each client and vendor. This was not something that was readily apparent, rather it was the investigator's opinion and instincts based on the tone and content of the writing between the Prime Suspect and other individuals. These did not come across as professional arms-length business relationships. In addition, one email document in particular appeared to show that some of the suspects and individuals external to the Company might be involved in defrauding the Company. It contained what appeared to be receipt and distribution of external funds after the Company made payments on transactions the suspects were involved in. Management needed to be told.

- **Initial Presentation of Findings – Week 3**

  The personal business being conducted was complex due to the number of individuals and entities involved. In addition to the strange relationships with individuals working for the clients and vendors, there were several other suspicious relationships. For instance, the Prime Suspect listed himself as Co-President of one of the vendor firms he/she did business with on proposals submitted to clients. Also, another vendor was listed as a client in proposals prepared for new clients and an employee of the Company was listed as a client of the Prime Suspects personal business, using the Company's name.

  In order to communicate these complex findings, a flowchart was developed that depicted the people, personal businesses, clients, vendors, and third party

[2] The untouched original versions of all copied information is stored in this directory. This data is then copied to a working folder where it is opened and reviewed.


"EXHIBIT 1.doc"

consultants involved in the Prime Suspect's personal businesses ( ). It also showed some of the more significant unusual relationships that existed between the Prime Suspects and vendors used.

Several boxed-in areas containing textual information were also provided listing integrity issues, areas requiring further investigation, and next steps. Certain steps were identified as a risk because taking them would require requesting information from other areas of the Company and would expose the names of the suspects under investigation to other parties. This could lead to the suspects finding out they were under investigation and subsequent destruction of vital electronic and paper records. We were especially concerned about electronic information that we wanted to forensically obtain.

Forensically obtained information has been accepted in the past in a court of law[3]. When forensically obtained information is absent, prosecution in a court of law, could be hindered and in some cases even prevented. This has occurred due to the change in the form of evidence from a historical paper format to an electronic format with a vast majority of information now being stored electronically. In some cases the information are never printed[4]. This therefore, could not be ignored. It became clear that it was very important to move the investigation along quickly in order to preserve the electronic evidence.

The flowchart was first presented to the Security Director. What happened over the next two days demonstrates the power of carefully crafted, concise information. The Security Director immediately decided that this should be presented to the V.P of the Business Unit where the suspects all worked. The next day, a presentation was requested for the Executive V.P. in charge of all Business Unit Services with a presentation to be given to the General Counsel beforehand. At the meeting with the Executive V.P., it was decided to fast track the investigation. This was based on the suspects' demonstrated disloyal activities and the expressed concern of the potential for system damage that these individuals could do, since six of the seven suspects had some of the highest privileged system administration access.

A meeting was held with a project team consisting of Audit, HR, Business Unit Management, Legal and Security. It was decided that the same information obtained for the Prime Suspect would be covertly obtained for each of the other suspects and that all other available information useful to the investigation would be

[3] Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639 (S.D. Ind. 2000) http://www.forensics.com/html/resource_case_involvement.html (May 1, 2004)

[4] Hastings, Glen. "5 Common Mistakes in Computer Forensics". Online Security, Jul 10 2003 http://www.onlinesecurity.com/Community_Forum/Community_Forum_detail133.php (May 4, 2004)

obtained and reviewed. We started with information available from the Business Unit Director as this would minimize exposing the suspects' names to others.

- **Round 1 – Investigative Analysis - Week 3 and 4**

  Copies of each suspect's mailboxes and hard drives were covertly obtained and saved as per investigation methodology. These were then reviewed and documented for each suspect. Land, cell, and calling card telephone records were obtained and reviewed and total minutes were summarized by calls to and from the personal businesses clients and vendors. Remote access activity for non-business use was also documented. Compliance documents signed by the suspects were obtained. Time sheets and billing documents of the Personal Business, showing the hours spent by Client, were totaled for each suspect.

  It was then agreed to schedule simultaneous interviews with all of the suspects, and at the same time, confiscate their computers for computer forensics[5] review, and search their work area for relevant documents and electronic storage media.

- **Interviews – Week 5**

  Available Information pertaining to each suspect was collected, summarized, and placed in a separate documentation binder. By the end of the investigation, each

  
  "EXHIBIT 2.doc"

  suspects' binder contained the information shown in

  
  "EXHIBIT 3.doc"

  Generic opening and closing statements ( ) were prepared for the interviews and specific questions for each suspect were developed based on research and analysis done to date. It was important to set the stage properly by informing each of the suspects of what we knew and what we expected from them in order to give them the opportunity to tell what they know and explain their actions. It was equally important to treat each suspect in the same manner, hence the generic statements.

  At the end of the interviews, the suspects were placed on administrative leave with pay and instructed not to talk with anyone but their manager about the investigation.

---

[5] Computer forensics is the collection, preservation, analysis, and court presentation of computer-related evidence. "Computer Forensics" WindowMeister.com, 2003 http://www.windowmeister.com/computer_forensics.htm. (May 2, 2004)

Simultaneously with the conduction of the interviews, the suspects' computers were seized. When confiscating computers a proven acceptable protocol must be followed. First, a chain of custody[6] must be established and maintained. In this case, one individual was assigned to coordinate picking up all of the computers and bringing them to a central location where he/she was required to sign-in each one. This was then counter-signed by one of the investigators. The computers were then placed in a locked area, within a locked room. This room was located inside an access-restricted office. The investigators then controlled access to this equipment throughout the investigation. Whenever a computer was released, it was signed-out by the retrieving individual and counter-signed by the evidence custodian.

Second, the method of retrieval must be done in such a way as to mitigate the potential for information loss. This was accomplished by following proven methods for seizing computer equipment[7]. In this case, all of the computers had power physically removed and were not powered down normally. This was done to ensure that nothing would be accidentally destroyed. It would also prevent auto erase of swap files[8], etc., that may be part of the machine's normal shutdown. This would also prevent activating the unlikely possibility that a machine was rigged to erase all data if a certain order is not followed or code provided during normal shutdown.

It is important to follow protocol throughout the investigation. This requires that the investigators be skilled experts in the field of computer forensics. Our investigators had over 4 years of forensics experience, and certifications from Guidance Software on Encase[9] versions 3 and 4, and from New Technologies, Inc[10]. on their forensic software suite.

A team meeting was held where the results of the interviews were discussed and next steps decided. Management now wanted a complete forensic review[11] of the suspects' computers and detailed information presented on each.

---

[6] A process used to maintain and document the chronological history of the evidence. "Glossary – Chain of Custody". http://peace-officers.com/content/glossary/def-chain.shtml (May 1, 2004)

[7] "Best Practices for Seizing Electronic Evidence Version 2.0." A Joint Project of the International Association of Chiefs of Police and the United States Secret Service http://www.secretservice.gov/electronic_evidence.shtml (May 4, 2004)

[8] A swap file (or swap space or, in Windows NT, a pagefile) is a space on a hard disk used as the virtual memory extension of a computer's real memory (RAM). Data is constantly written to and read from this memory extension. "Definitions – Swap File" http://whatis.techtarget.com/definition/0,289893,sid9_gci213077,00.html (May 2, 2004)

[9] www.encase.com

[10] http://www.forensics-intl.com

[11] Patzakis, John. "Computer Forensics as an Integral Component of the Information Security Enterprise". Guidance Software, 2003. http://www.guidancesoftware.com/corporate/whitepapers/downloads/computerforensics.pdf (May 4, 2004)

- **Round 2 – Extensive Detailed Analysis – Week 5 & 6**

  Forensic acquisitions, research, and analysis were performed on each suspect's computers. There were 26 computers confiscated and most would require having forensic acquisitions performed over the six-week period. As a result, thousands of pages of documentation were printed and compiled into a separate documentation binder for each suspect, and multiple copies were made so team members would be able to review in their offices.

  At the next team meeting, management requested that the information be summarized so comparisons could be made on the degrees of involvement of each of the suspects. At this stage much of the team felt that of the seven individuals involved, only one or two would be dismissed. The author, however, was sure that, based on our findings to date, at least four of the seven were so intricately involved with the "side-business" that they would eventually be dismissed, if the information was presented in an understandable way and was fully comprehended. A means of clearly communicating these findings needed to be created.

  A spreadsheet was developed depicting the seven suspects' Emails, telephone, VPN, instant messaging, and non-business computer usage, etc.

  

  "EXHIBIT 4.xls"

  ( ). Color-coding was used to highlight column and row headings, and to improve ease of reading.

  This summary information was then presented to the team, and each suspect was discussed at length. The presentation format of the information clearly showed the different levels of involvement by each of the suspects. The strategic use of numbers, dates, percentages, and text revealed, in a straightforward manner, how each subject spent many hours working on the personal business, while on Company time.

  Based on this review, it was decided that the Initial focus going forward would be on the two individuals with the least involvement, so their fate could be decided quickly. It appeared that their involvement would not warrant dismissal. This was done out of consideration for the individuals and out of management's desire to minimize the impact of the absence of so many high-level technical people. It was also felt that this type of quick action would assist with employee morale within the affected department.

  A computer forensics review of their hard drives confirmed that these two individuals had the least involvement and could be brought back to work the next week, the sixth week of the investigation, but just 10 days after they had been put on administrative leave. For the other individuals more complete information was requested. This information would be obtained by performing extensive computer forensics reviews.

The presentation of the summary information allowed management to make an early-on decision to bring back two employees whose role in the personal business had been minor.

The spreadsheet helped solidify opinion about the extent of the other individuals' involvement. Team members were now inclined toward dismissal for 4 of the other 5 suspects. Suspect 3 had only light involvement based on many of the categories investigated. Many of the team members felt that we would lose on appeal if this individual were dismissed, even though this individual was not helpful or forthcoming during the interview.

The computer forensics review for each of the individuals confirmed their participation and provided a wealth of documents in support of the extensive involvement for 4 of the 5 individuals.

The forensic review of Suspect 3's computer provided evidence of a deliberate attempt on his/her part to interfere with and obstruct the investigation. Over 40 files, which specifically pertained to the investigation, were found to have been deleted by this individual just prior to his/her interview, but after he/she had been informed that an investigation was underway. This was a direct violation of the Ethics Standards, and in fact was part of the generic statement read to each of the suspects at the interviews.

.

This had happened because Suspect 3 was on vacation the day of the scheduled interviews and he/she had his/her laptop with him. He/she was contacted by his/her manager, told about the investigation, read the generic introduction statement, and asked to report to his/her Manager as soon as possible. He/she was told to turn in the laptop at that time.

- **Investigation Summary**

This investigation was very complex, involving a number of employees stealing time, and in some cases, money from the company. Frequently, for a number of legitimate reasons, an investigation can be moved too quickly in order to mitigate both employee morale issues and potential bad publicity. This can jeopardize the investigation.

At the same time, certain investigations need to be fast-tracked because of the potential downside of moving too slowly. In this case, it was important to move quickly because these individuals had the highest level of privileged system access and could do considerable damage if they chose. Employee morale was a factor given that the seven employees were all from the same department and were all technical experts in their areas. The Department management had made it clear that these events had brought great consternation and stress to the remaining department employees.

By using creative presentation tools the investigators were able to focus management's attention on the need to provide the proper resources and move quickly toward a conclusion that was best for the organization. A key example was the flowchart Exhibit 1. This tool resulted in quick attention being paid to the initial findings, and decisive action being taken, and the investigation being fast-tracked.

We were asked how we could move the investigation along faster. We indicated that limiting factor was our forensic capability. This was because each acquisition and analysis would take days, and we had only two forensic machines and needed to perform numerous forensic acquisitions and reviews. We asked for and received approval for immediate doubling of our forensic acquisition capability. Two more Forensic computers and two more copies of forensic software were purchased at a cost of $20,000.

The presentation tools helped to highlight the individuals' activity and provided summary data on their actions. Management was able to fully understand the extent of what had happened and take the necessary decisive actions. It was also determined that the Prime Suspect and one individual at each of three clients and two vendors were involved in defrauding the Company and the clients of the Prime Suspect's personal business.

As a result of this investigation, five employees were terminated. Others were given a written warning or provided with coaching and counseling.

- **Documentation**

Once an investigation has been brought to its conclusion, an Executive Report[12] is prepared and communicated to Company management. This report is a standard format that provides an executive and detailed summary of the investigation facts,

"EXHIBIT 5.doc"

findings, and recommended corrective and preventive measures ( ). The objective is to highlight the critical facts and actions so an executive can quickly absorb what happened and what was done.

The most important section is the prevention and correction action plan. Its prime purpose is to identify the control weaknesses and the necessary deterrents and improvements that need to be implemented. It also serves as a tracking mechanism by providing a responsible party and agreed to completion date.

- **Conclusion**

[12] Company Investigative Services Group. "Executive Report template" 10/31/03

In conclusion, the reader should see the value of clear, concise, and creative presentation tools when briefing management on complex investigations[13]. They help to frame the decision-making and allow for quick and decisive action, with what is usually a slow moving process, by a very deliberate management.

The following happened as a result of the presentation tools used with this investigation:

- The investigation was immediately brought to the attention of top management.
- The investigation was fast-tracked and necessary staffing and other resources assigned.
- Each suspect's level of participation was revealed and this allowed management to focus on initially bringing those with minor involvement back to work.
- Attention was focused on those who needed more extensive review.
- One suspect was identified as needing more research.
- Documented the case against each suspect in an organized fashion.
- A written summary of the investigation was provided as well as a tool for identifying preventative and corrective actions as well as a means of following up that the necessary actions were implemented.

A list of the hardware and software tools used to conduct this investigation and create the presentation tools is contained in Attachment A below.

[13] Two sites the reader may find useful when creating charts:
http://www.state.sd.us/deca/DDN4Learning/ThemeUnits/Charts/index.htm
http://user.training.apple.com/demo/keynote/segment101065.html

References

[3] Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639 (S.D. Ind. 2000 http://www.forensics.com/html/resource_case_involvement.html (May 1, 2004)

[4] Patzakis, John. "Computer Forensics as an Integral Component of the Information Security Enterprise". Guidance Software, 2003. http://www.guidancesoftware.com/corporate/whitepapers/downloads/computerforensics.pdf (May 4, 2004)

[5] Computer forensics is the collection, preservation, analysis, and court presentation of computer-related evidence. "Computer Forensics" WindowMeister.com, 2003 http://www.windowmeister.com/computer_forensics.htm. (May 2, 2004)

[6] A process used to maintain and document the chronological history of the evidence. "Glossary – Chain of Custody". http://peace-officers.com/content/glossary/def-chain.shtml (May 1, 2004)

[7] "Best Practices for Seizing Electronic Evidence Version 2.0." A Joint Project of the International Association of Chiefs of Police and the United States Secret Service http://www.secretservice.gov/electronic_evidence.shtml (May 4, 2004)

[8] A swap file (or swap space or, in Windows NT, a pagefile) is a space on a hard disk used as the virtual memory extension of a computer's real memory (RAM). Data is constantly written to and read from this memory extension. "Definitions – Swap File" http://whatis.techtarget.com/definition/0,289893,sid9_gci213077,00.html (May 2, 2004)

[9] www.encase.com

[10] http://www.forensics-intl.com

[11] Patzakis, John. "Computer Forensics as an Integral Component of the Information Security Enterprise". Guidance Software, 2003. http://www.guidancesoftware.com/corporate/whitepapers/downloads/computerforensics.pdf (May 4, 2004)

[12] Company Investigative Services Group. "Executive Report template" 10/31/03

[13] Two sites the reader may find useful when creating charts:
http://www.state.sd.us/deca/DDN4Learning/ThemeUnits/Charts/index.htm
http://user.training.apple.com/demo/keynote/segment101065.html

Attachment A

Hardware & Software Tools

Hardware

- Digital Intelligence (http://www.digitalintel.com/)
  - Forensic Recovery Evidcence Device (FRED)
  - Forensic Recovery of Evidence Device Diminutive Interrogation Equipment (FREDDIE)

- Forensic_Computers (http://www.forensic-computers.com/products.html)
  - Forensic Solid Steel Tower (with Dual AMD CPU)

- Hewlett Packard (http://h18006.www1.hp.com/products/storageworks/dltvs4080/index.html)
  - SureStore DLT vs80 Tape Device – Used for Backups

Software

- Guidance Software(www.encase.com)
  - Encase Forensic Software versions 3.22f and 4.07

- Pacestar Software (http://www.pacestar.com/wizflow)
  - Wizflow Flowcharter version 4.15

- Microsoft (www.microsoft.com)
  - Windows 2000 Professional version 5.0 and XP Professional version 5.1 Operating Systems
  - Microsoft Word 2002 version 10.26
  - Microsoft Excel 2002 version 10.26
  - Microsoft Outlook 2002 version 10.26
  - Microsoft Internet Explorer version 6.0

- NovaStor (www.novastor.com)
  - Novaback+ version 6.7

Last Updated: July 23rd, 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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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
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 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
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor