Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Running an IT Investigation in the Corporate Environment

This paper describes the issues that are involved in conducting an IT investigation of an incident in a corporate environment. It helps to provide insight into the issues that many companies deal with when it comes to ensuring that an investigation is done correct. The paper starts by describing hurdles that many IT investigators face and gives solutions to help overcome these problems. This paper will help you understand the need for creating severity guidelines in your organization so that an incident can be assessed...

Copyright SANS Institute
Author Retains Full Rights

AD

**Security Essentials Certification (GSEC)**
**Practical Assignment**
**Version 1.4b**

# Running an IT Investigation in the Corporate Environment

**Carl F. Endorf, CISSP**

**Abstract**:

This paper describes the issues that are involved in conducting an IT investigation of an incident in a corporate environment. It helps to provide insight into the issues that many companies deal with when it comes to ensuring that an investigation is done correct. The paper starts by describing hurdles that many IT investigators face and gives solutions to help overcome these problems.

This paper will help you understand the need for creating severity guidelines in your organization so that an incident can be assessed and investigated properly as well as communicated correctly. In addition, this paper helps outline the basic steps in properly conducting and investigation, including knowing how to rate the severity and potential risk that the particular incident may pose.

## Introduction

In a study conducted annually by the Computer Security Institute and FBI on computer crime, only 74% of 2000's survey respondents acknowledged that they had suffered a financial loss due to computer incidents [CSI 2000]. In addition, only 42% of the respondents could put any monetary value on the incident. Consequently, the $265,589,940 dollars reported by the survey as lost, is much lower than what is actually happening. The same survey in 2001 shows that 91% of the respondents acknowledged financial losses resulting from computer incidents. A more recent report from The Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad, April 2002 shows that 90% of the companies detected employee abuse of Internet access privileges. In addition, research shows that for the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).

One reason corporations have a difficult time stopping computer crime and abuse is that there is very little good information about what computer crime is and how it can be investigated in the corporate environment. There are many roadblocks that will hamper the investigative process and many misunderstanding along the way.

## Understanding the Issues

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

One of the problems in the corporate arena is a lack of understanding of the skills and people needed for corporate IT investigations. The physical security and auditing departments typically have the investigative and legal background, but lack the IT skills or proper understanding of the network that the IT folks do. In addition, the problem with the IT folks is that they lack the investigative skills to do the job right by preserving the evidence and not overwriting the valuable information that exists for a thorough investigation. Unfortunately, most companies have little if any communications and knowledge sharing between the two groups.

Another aspect is that companies face is that much of the documentation and training today is geared for law enforcement. Law enforcement has a much different goal in mind when they conduct an investigation- a conviction! That is one of the last things that many corporations want, they are interested in keeping their reputations in tact and getting back to business. A conviction will many times bring more monetary harm in the way of reputation to the company than is worth their effort. There is a plethora of information on doing criminal investigations for law enforcement, but the porting of that information to corporate investigations is only just beginning.

A third issue is that the business need many times gets in the way of the investigation. There may be a web server that has valuable evidence to help in an investigation, but if there is no redundancy for that server and the company cannot, or will not, take it down as it is crucial to the operation of the business, your investigation is halted and the evidence is overwritten. The frustration the investigator feels needs to be put aside by the fact that the business is there to do business and not for the IT investigator. But a caveat to this is that the business side needs to realize that the cost of letting these security incidents continue will cost the company not only lost business productivity, but a loss of reputation and a possible spot on the evening news! In fact as we have seen in the past with companies like CD Universe the loss of reputation can be the worst possible type of incident that a company can endure and lead to your companies demise. Think it will never happen? Neither did any of the number of companies that went under because of this in the past year!

The final issue is dealing with other departments while investigating your own employees. Most human resource departments know what to look for when there are issues with excessive absenteeism or poor work habits, but not computer abuse. In addition, many corporate legal departments may also struggle with technology and what the threats and the constantly changing legal issues surrounding it. After all, with the high demand for technically savvy lawyers it is likely most corporations have none well versed in cyber law, and if they do, they are overworked and do not have the time to put into your IT investigations.

**Overcoming the problems**

The first way to overcome these problems is to communicate and educate management and their respective departments. Have a Point of Contact (POC) in each department including Legal, Auditing and Human Resources and create a steering

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

committee with a collaborative database, or use your existing Computer Security Emergency Response Team [RFC 2350], if you have one, to help facilitate the investigations. Pass ideas back and forth, share experiences and learn from each other. Attend technical and investigative workshops at the same time and or share that information with all parties involved. Get a non-disclosure in place with a non-competing company that is set up similar to yours and share your experiences. The more familiar the departments are with each other the easier it will get to lean on each other and learn. In addition, it is important that all areas are educated. Have the people doing the investigations trained on both technologies needed to do the job right and the skills to properly investigate, such as chain of custody and preservation of evidence. You can have a class for the Human resource department on what capabilities your investigative team has and help them to understand the basics of computer technology and how you investigate them.

In addition to educating the business side it is important that you create a proper method to evaluate the risk in which the potential crime or incident posses. You will need to take into account both the technical and business aspects of the incident. For example, you may already have a system in place to evaluate other non-IT security issues and to evaluate business risk, adapt these to fit into your incident severity guidelines. (See figure 1.) For an example loosely based on the CIAC Incident procedures, on assessing the risk of an event.

| Incident Severity Guidelines | | | | |
|---|---|---|---|---|
| **Priority Guidelines** | **Rating** | **Initial Action Guideline** | **Resolution Goal** | **Ownership Acknowledged** |
| **Level 4**<br>Severe impact on our ability to perform a segment of our business | 13-15 | Immediately | ASAP | Immediately |
| **Level 3**<br>A total loss of major service to a business group or application<br>SLO is impacted | 11-12 | Immediately | < 24 hours | Immediately |
| **Level 2**<br>All general problems that have an impact on business partners or groups<br>No service level impacts | 8-10 | Within 5 hours | < 72 hours | < 3 hours |
| **Level 1**<br>All general problems or questions that have minor impact on business partners or groups. Minor impact on service | 5-7 | Within 24 hours | < 7 days | < 6 hours |

**Figure 1. Incident Severity Guidelines**

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The following are definitions of some of the variables that a company may want to include when formulating severity levels:

**Potential number of business partner's affected-** who is this incident affecting right now? One person, one group, several groups the entire enterprise.

**Probability of widespread escalation-** probability of spreading to a subnet, or the enterprise?

**Probability of use vulnerability-** though the vulnerability exists, how likely is this to happen. Consider difficulty and commonality.

**Potential for Damage/Loss-** estimated financial impact on State Farm. We want to look at the worst case and best case scenario and use the median of that to determine the range. This will require the input of the business partners.

**Business Impact-** this is the impact on our customers, down time and delay of critical projects.

Once you have determined the crucial variables needed to assess your risk, put them in a form that can be evaluated (see figure 2.).

| Severity Formula | | |
|---|---|---|
| **Factors** | **Rating** | **Score** |
| **Potential number of business partners affected** | **1= One system/person<br>2= More than one less than ten systems/people<br>3= More than 10 systems or people** | |
| **Probability of widespread escalation** | **1= Minimal 2=medium<br>3=High** | |
| **Probability of vulnerability use** | **1= commonly happens 2= occasionally happens<br>3=Can be done, but difficult and rare** | |
| **Potential for Damage/Loss** | **1= Minimal 2=medium<br>3=High** | |
| **Business Impact** | **1= Minimal 2=medium<br>3=High** | |
| **5-7 = Level 1 incident<br>8-10= Level 2 incident<br>11-12= Level 3 incident<br>13-15= Level 4 incident** | **TOTAL =** | |

**Figure 2. Incident Severity Formula**

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

These severity-rating systems are highly customizable to your companies' needs and issues. They should allow for the consideration of both the investigative/technical and the business issues. This allows upper management to look at a more balanced view of the risks associated with the issue.

**Conducting the Investigation**

The first thing to be considered is deciding on what an incident is. This can vary depending on the organization, but should include some of the following guidelines:

1. Unauthorized Access. All attempts at unauthorized access, whether or not they are successful, even if unauthorized access is suspected but not proven.

2. Malicious Code. Instances of malicious code such as viruses, Trojan horses, or worms.

3. Denial of Service. Denial of service (successful or unsuccessful) that affects or threatens to affect a critical service or denies access to all or large portions of a site's network.

4. Scans and Probes. Unauthorized network scans, probes, and attempted denial of service.

The analysis of the damage and extent of the incident can be quite time consuming, but should lead to some insight into the nature of the incident, and aid investigation and prosecution. As soon as the breach has occurred, the entire system and all of its components should be considered suspect. System software is the most probable target. Preparation is key to be able to detect all changes for a possibly tainted system [RFC 2196].

Once the correct people have been identified and trained, as well as the communication being opened up between the investigative team and other areas, it is essential to have the proper steps to take to conduct your investigation. It is important to note that depending on the incident each step may or may not take on more or less importance. The following steps will help the corporate investigator most effectively and thoroughly get the job done:

1. Eliminate the obvious
2. Understand the attack
3. Reconstruct the event
4. Trace the event back to the source
5. Analyze the source information
6. Gather the evidence
7. Hand over the evidence

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The first thing to do is to eliminate the obvious, this can be one of the most important things you can do, as in many cases much time will be saved if you rule out the obvious. Start with the technical people and see if they have changed anything recently. Is there any technical reason this would happen? Many times when you are investigating an incident people tend to be alarmists and over react, while it could be from a normal process or human error.

If you have ruled out all obvious possibilities then the next thing to keep in mind is that you need to understand the attack and where could it have come from. Remember to examine all possibilities. Before we go much further it is important to discuss some common types of computer attacks:

- Military and intelligence attacks made by espionage agents to gain classified information.
- Financial attacks made on banks may be professional criminals or amateurs.
- Business attacks made by competitors to gain competitive information.
- Attacks made by terrorist on government computers to cause damage or harm.
- Angry employees or ex-employees can conduct Grudge attacks on companies.
- Individuals for the intellectual challenge or fun make "Fun" attacks.

You want to try to understand how the person may have broken in or done what ever it is they did. This may seem obvious in some cases, like if someone sends an insulting email to the company CEO, you can look at the email headers to figure where it came from. However, this may go much deeper than that and you may need to contact the ISP or see if the email came from a remailer or was spoofed. This is the point when you may want to give Legal or HR a call and let them know what is going on. It is important to let them in on things early as not to surprise them and catch them unprepared.

Once you have a hypothesis of how the attack happened you would want to try to reconstruct the events that may have taken place. Using the same incident as earlier with the threatening email, how did the bad guy send it? The ***From:*** line says that it came from GWBUSH@whitehouse.gov, but the email headers show more. The IP indicates another source. So now, maybe we can reconstruct what may have happened here. Someone may have used some sort of fake mail program to spoof the ***From:*** line in the email to look like it came from someone it did not.

Now we have reconstructed the event and can try and to trace it back to its source. Since we know the IP address that the email came from, we can do a *whois* command and find out the owner of that IP range or address. Lets say we find out that it came from *ficticiousISP.net*, we can now try to see if the person is listed in the member directory, contact the ISP or at the very least be assured that the mail is not from the president of the United States.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Once traced back to the source it is time to analyze the source that it came from. Does the information on the machine support the original hypothesis? Is there any contradicting evidence? This is the point when you know if you have gone in the right or wrong direction. If the wrong direction was chosen log what you have done and start the process again starting at step 2 or three.

Now is the time when you want to gather as much data about the event as possible and log it step by step. Your organization will want gain as much knowledge about the event as possible. Your goal may not be to prosecute, but it never hurts to follow the procedures as if you were. Log everyone involved, what they did and the reasons why. Remember you may not be the only ones involved, you may have been a launching pad for other attacks for the bad guy, and may end up going to court. So, make sure you have everything in order. Following are an example of some of the questions that need to be asked:

**How?**
- How was access gained? What vulnerability was exploited?
- How was the incident detected?

**What?**
- What type of information was the compromised system processing?
- What service did the system provide (DNS, key asset servers, firewall, VPN gateways, IDS)?
- What level of access did the intruder gain?
- What hacking tools and/or techniques were used?
- What did the intruder delete, modify, or steal?
- What unauthorized data collection programs, such as sniffers, were installed?
- What was the impact of the attack?
- What preventative measures have been (are being) implemented?

**Who?**
- Determine responsible party's identification, usually IP address(es) or host name(s).
- Does the compromise involve a country on the DOE Sensitive Country List?

**When?**
- When was the cyber security incident detected?
- When did the cyber security incident actually occur?

Finally, this is the time when you can hand over all the documentation to the Legal Department and Human resources to for a decision to be made. This will depend on many factors such if the attack was internal or external and the extent of the attack. This should not be the decision of the investigative team, they are there for just what their name says, investigations.

**Conclusion**

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Although there are many bumps in the road to a good IT investigation, this paper has attempted to show just some of the ways in which they can be overcome. This includes the communication and education of business partners, management and ourselves. In addition, we need to have demonstrated the necessity of severity through a severity model in order to rate how we want to proceed with the investigations, and to what scale. Finally, we discussed the proper steps to take when conducting an investigation.

It is important that companies become more streamlined in their goal of conducting proper IT investigations, because the problem is growing rapidly. We need to be prepared for increasing computer attacks and abuse as companies become increasingly dependent on technology. Information warfare is not only limited to government anymore, we need to be prepared to investigate the sources in which our information is getting out, whether that be from inside or outside the company.

So, where do we go from here? We plan, educate and cooperate with in our own organization for the types of intrusions that we will be facing. We have the steps in place before the incidents occur and we make ourselves ware of the potential harm that we are susceptible to.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

**References**

*1. [CSI 2000] [CSI 2001] [CSI 2002] CSI Computer Crime and Security Survey, Copyright 2001 © Computer Security Institute1999, 2000, 2001*
http://www.gocsi.com/press/20020407.html

*2. [RFC 2350] Expectations for Computer Security Incident Response, RFC 2350, author N. Brownlee Et al., 1998 The University of Auckland.*

*3. [RFC 2196] Site Security Handbook, RFC 2196, author B. Fraser, 1997,Category: Informational.*

*4. Investigating Computer-Related Crime, Peter Stephenson, CRC press, Copyright 2000 ©, ISBN # 0849322189*

*5. The IT Security Professional as Investigator, David Morrow. Ernst and Young LLP, 2002*
http://www.gocsi.com/sec.pro.htm

*6. Karnow, Curtis E.A. "Recombinant Culture: Crime in the Digital Network." Paper presented at Defcon II, Las Vegas, July 1994. Available at:*
http://www.cpsr.org/cpsr/privacy/crime/karnow.html

*7. Fighting Computer Crime, David Icove, Karl Seger, and William VonStorch, December 02, 2002*
http://www.crime-research.org/eng/library/crime1.htm

*8. Hackers target government and companies , Computer Crime Research Center, November 27, 2002,*
http://www.crime-research.org/eng/news/2002/11/Mess2702.htm

© SANS Institute 2003, Author retains full rights

Last Updated: September 2nd, 2015

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Crystal City 2015 | Crystal City, VAUS | Sep 08, 2015 - Sep 13, 2015 | Live Event |
| SANS Network Security 2015 | Las Vegas, NVUS | Sep 12, 2015 - Sep 21, 2015 | Live Event |
| SANS Seoul 2015 | Seoul, KR | Sep 14, 2015 - Sep 19, 2015 | Live Event |
| Data Breach Investigation Summit & Training | Dallas, TXUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Baltimore 2015 | Baltimore, MDUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Perth 2015 | Perth, AU | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Tallinn 2015 | Tallinn, EE | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS ICS Amsterdam 2015 | Amsterdam, NL | Sep 22, 2015 - Sep 28, 2015 | Live Event |
| SANS Bangalore 2015 | Bangalore, IN | Sep 28, 2015 - Oct 17, 2015 | Live Event |
| SANS DFIR Prague 2015 | Prague, CZ | Oct 05, 2015 - Oct 17, 2015 | Live Event |
| SANS Seattle 2015 | Seattle, WAUS | Oct 05, 2015 - Oct 10, 2015 | Live Event |
| SANS Tysons Corner 2015 | Tysons Corner, VAUS | Oct 12, 2015 - Oct 17, 2015 | Live Event |
| SOS: SANS October Singapore 2015 | Singapore, SG | Oct 12, 2015 - Oct 24, 2015 | Live Event |
| SANS Gulf Region 2015 | Dubai, AE | Oct 17, 2015 - Oct 29, 2015 | Live Event |
| SANS Cyber Defense San Diego 2015 | San Diego, CAUS | Oct 19, 2015 - Oct 24, 2015 | Live Event |
| SANS Tokyo Autumn 2015 | Tokyo, JP | Oct 19, 2015 - Oct 31, 2015 | Live Event |
| SANS South Florida 2015 | Fort Lauderdale, FLUS | Nov 09, 2015 - Nov 14, 2015 | Live Event |
| SANS Sydney 2015 | Sydney, AU | Nov 09, 2015 - Nov 21, 2015 | Live Event |
| SANS London 2015 | London, GB | Nov 14, 2015 - Nov 23, 2015 | Live Event |
| Pen Test Hackfest Summit & Training | Alexandria, VAUS | Nov 16, 2015 - Nov 23, 2015 | Live Event |
| SANS Hyderabad 2015 | Hyderabad, IN | Nov 24, 2015 - Dec 04, 2015 | Live Event |
| SANS Cape Town 2015 | Cape Town, ZA | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| SANS San Francisco 2015 | San Francisco, CAUS | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| SANS Milan 2015 | OnlineIT | Sep 07, 2015 - Sep 12, 2015 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |