Global Information Assurance Certification Paper

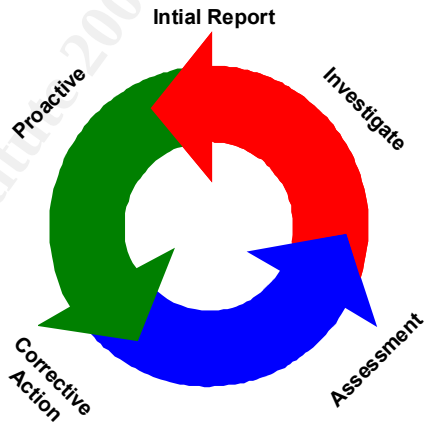
Wendy Branson
GSEC Version 1

The Security Continuum of Incident Management

OVERVIEW

In our current climate of terrorist activities and cyber attacks, corporate policies must focus even more on computer security and incident response plans. Given the financial losses from customers and investors that could result from an internal or external breach, organizations need to be doing more in the way of awareness and prevention. By spending the money and developing the processes up front, they can repel an attack or respond to it more quickly.

Key to this is the development of an incident handling process. The Security Continuum serves as a model for developing a process for incident handling and provides the guidance before and after an incident occurs. The diagram of the Security Continuum [i] is a clockwise circular flow, where each phase acts as a continuation of the previous phase, and predecessor of the next.



Phases of the Security Continuum

Initial Report

The security continuum begins with the report or an incident or anomaly. There are various ways this can occur: a customer, an employee or intrusion detection system that triggers the initial report. The Information Security Department (ISD) should be able to receive the report over the phone, via email or a web site, with each of these processes allowing for anonymous reporting. These services should be advertised via a security awareness program.

Didn't we all learn in school the 6 P's - Proper Prior Planning Prevents Poor Performance? A few key items like a notification list and procedures highlighting what should be done when an anomaly is reported are part of this initial phase.

A central contact point in ISD should be defined who is knowledgeable in the structure of the business and has excellent computer and customer service skills. They must also understand that all reports must remain confidential. Without confidentiality the investigative process may be hampered and the company is as risk of wrongfully accusing an employee of policy violation or criminal acts.

Key to the strength of this first phase is strong documentation during the evolving incident response. As any good investigative reporter can tell you, by asking "who, what, when, where, why, and how" the initial report should be able to generate an overview of the anomaly. A standard form should be developed to ensure that each incident is handled property and all necessary questions are asked and information is recorded. The report should also serve as the baseline to determine if and when the investigative process begins and ends. Should it be determined that the anomaly will not be pursued, it can serve as a record of the incident.

- A thorough investigative should begin with the "***who***" questions. Who is the person making the report, who is the witnesses and finally who are the victims? The victims would include the owner of the application, system administrators and other associated groups.

- The "***what***" questions would address a description of the anomaly and the environment. What are the conditions that were identified? What system(s) was this identified on? The reported must also identify the importance of the application to the business. It is important to determine that if the anomaly is found to be a true incident, whether it would have a direct financial or shareholder impact.

- "***When***" would include the time the anomaly was discovered, and when it is suspected that it occurred. There will likely be a difference in time when the suspected anomaly was identified and occurred, but by utilizing system logs or other tools, the reporter may be able to determine when the incident occurred.

- The "***where***" questions would entail the where the anomaly occurred, the location of the affected system, and location of the reporter. Quite often the person who reports the anomaly may be a user of the system, and not in the same location as the actual system. At this point, it may not be clear whether what is being reported is the actual incident or merely a response to the incident.

- The reporter may also be able to provide some insight as to "***why***" they think the anomaly occurred. Could it be a disgruntled employee or customer? If a web site is defaced, did it provide any clues as to whether it was political statement? Are there financial problems or layoffs occurring at work?

- And finally "***how*****"** the reporter feels this happened. The steps taken by the reporter to arrive at this conclusion must be clearly documented. If the investigation of the anomaly proceeds, a through understanding of how their steps could have impacted the trail will require thorough understanding and documentation.

Investigative

A very basic assumption here is that the company has thoroughly communicated a policy regarding the approved use of business resources. Without this, there is no legal basis for monitoring or investigations can take place. The employee policy on overall computer security, which may include the company's position on misuse of systems and prohibited activities should be broad enough to cover all uses of the corporate resources and clearly communicate what is and is not appropriate use. It must also state that violations of the policies are regarded as illegal activities and can result in the monitoring and involvement with law enforcement agencies. Employees, contractors and other business associates should be required to review the policies periodically and initial their acceptance and understanding.

The first step of the investigation process is to identify which computer media(s) may contain evidence, which can be a painful and time-consuming process. When looking for a coin dropped in the grass, you can spend a lot of time, and find other items before finally locating the coin. So rather than looking for a particular thing on a computer, you'll want to step back and examine everything. An intruder doesn't display atypical behavior – they utilize odd commands or do things the normal users don't.

A knowledgeable computer forensics professional can have one major advantage over an intruder - knowing what your systems normally look like. The forensics expert should have experience on a wide range of computer hardware and software.

Basic computer hardware design and software implementation is often quite similar from one system to another, and experience in one application or operating system area is often easily transferable to a new system.

Electronic data includes records, files, programs, computer manufacturer specifications, and other footprints on a computer storage device. Because of the diverse application of computers in our society, this evidence can take many forms. It can include word processing documents, financial information, e-mail routed via the Internet/Intranet, personnel records, customer lists, electronic scheduling systems and computer operation logs.

Unlike paper evidence, electronic evidence can often exist in many forms, with earlier versions still accessible on a computer disk. Knowing the possibility of the existence of earlier versions, even alternate formats of the same data can be discovered.

So when does an anomaly become an actual incident? From the intelligence gathered during the initial phase of the investigation, a determination should be made if it appears to be an actual incident of unauthorized activity. Not every anomaly is the result of a dishonest act. The deletion of a file may be an honest mistake, and not worthy of a full -scale investigation. Instead, a record of the incident should be made, and this process should proceed to the corrective phase.

A decision must also be made to determine if the activity will be stopped immediately or monitored while additional evidence is gathered. There are many factors to consider with the most important factor being the impact to the business should the activity continue. If those involved in the investigative process feel the activities can be monitored accurately with no potential damage, monitoring should continue to build additional evidence. If not, the activity should be shut down immediately.

Recognizing the fragile nature of digital data, the second major task is to preserve the evidence against accidental or intentional manipulation. *Protection of evidence is critical.* A forensically sound examination is one conducted under such controls that it is completely documented, repeatable and the results are verifiable. Regardless of who completes an examination of the media and the specific tools and methods employed, if they use forensically sound tools and methodologies, they should get the same results. Timing is also a factor. Evidence vanishes over time, either as the result of normal system activity or as the actions of users.

The third step is to conduct an examination either directly on the image or use the image to make another copy of the media to be examined. Most professionals prefer to make a comprehensive image for this examination to ensure that no modifications are made to the original device. How this image is

examined is entirely dependent on the facts and circumstances of the specific case at hand, and the tools selected for the imaging process. To develop an accurate picture of what has changed, a baseline for the affected system prior to the incident can be an effective tool. It maybe possible to load this to determine what updates have been made. Even if this is not successful, the baseline can be used later during the corrective phase for comparison when correcting the system.

A knowledgeable forensics professional will ensure that the subject computer system is carefully handled to ensure that:

- no possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer.
- no possible computer virus is introduced to a subject computer during the analysis process.
- all files are discovered and recovered (to the extent possible) including deleted, hidden, temporary, swap, password-protected files, and encrypted files.
- a continuing chain of custody is established and maintained.
- business operations are affected for a limited amount of time, if at all.

Assessment

During the Assessment Phase, the ISD now has enough information to know what has been done, but needs to perform a thorough examination of the data to determine what action they might take. They also need to determine what other vulnerabilities might exist as a result of these activities. As many recent worms and viruses have shown, the initial attack can often leave a back door, which can be compromised by a later attack if left undetected.

An overall analysis of the subject computer system must be provided, as well as a listing of all possibly relevant files and discovered file data. The analysis should also provide an opinion of any attempts to hide, delete, protect, encrypt information, and anything else that has been discovered and appears to be relevant to the overall computer system examination. The actual and/or perceived damage to the system should also be presented. These factors will determine what level of criminal or civil proceedings may be pursued.

Corrective

Once the assessment has been completed, the ISD must present their findings to the decision-maker so they may take action. In some cases, the decision-maker is a corporate CEO or CIO. In other cases the decision-maker is involved in the criminal justice system, but not all cases will be turned over to the criminal or civil

process. This phase typically begins with the involvement of law enforcement or an interview by the ISD.

During the interview, the primary question on everyone's mind is why the suspect engaged in the unauthorized or criminal activity. During the interview the ISD should review the "who, what, when, where, why, and how". The suspect should be asked to focus on what changes they made to the system, when did they first attempt or succeed in their activities, and what their goal was in these activities. All comments should be documented in written form, which should be signed and dated when completed. The form should also document that no promises were made to the suspect in return for their statements, and the statements can be used as the company sees fit.

Many types of criminal and civil proceedings can and do make use of evidence revealed by computer forensics specialists. Criminal Prosecutors use incriminating documents found on computers as evidence in their prosecution of crimes. Corporations use forensic evidence relating to sexual harassment, embezzlement, theft or misappropriation of trade secrets, trading violations and other internal/confidential information. A civil litigation can use personal and business records found on computer systems that relates to fraud, divorce, discrimination, and harassment cases.

Proactive

To complete the Security Continuum, the ISD must perform a post-mortem. During this meeting all phases of the continuum should be reviewed with all parties involved in the process. An overview of the incident and observations of each phase from the incident report, investigation, analysis and corrective actions taken should be documented and provided to management. The ISD should focus on problems that were encountered and lessons learned, and these should be incorporated in the security awareness programs.

This is also a good point to focus on how other proactive measures could be taken to prevent another incident. Identification of system updates and monitoring of system alerts and bulletins can eliminate potential holes in the security defenses. Monitoring of chat rooms, message sites and trading sites can be excellent ways to detect potential leaks of information or preludes to potential violence.

Conclusion

Using the Security Continuum to develop an incident-handling plan will ensure a comprehensive examination from beginning to end of an incident. It also helps us to come "full circle" and ensure that the lessons learned from an

incident will be use to strengthen and improve the security policies and procedures.

---

[i] Information Security Management Handbook 4th Edition Harold F. Tipton, Micki Krause

Computer Forensics Expert Witness – Judd Robbins
http://www.computerforensics.net/forensics.htm

Forensic Computing
http://www.forensic-computing.com/archives/fundamentals.html

SC Magazine
http://www.scmagazine.com/scmagazine/2001_04/cover/cover.html

SC Magazine
http://www.scmagazine.com/scmagazine/2000_09/survey/survey.html

Questions: The answers are in bold test

1) The Security Continuum for Incident Handling is comprised of how many phases?
   a) Three
   b) Four
   c) Five
   d) Six

2) The Security Continuum flows in what direction?
   a) Vertical
   b) Counter clockwise
   c) Horizontal
   d) **Clockwise**

3) What basic questions should be answered in the initial report of an anomaly?
   a) Who, what, where, why
   b) When, how?
   c) How, who, with, when, where, why?
   d) A & B
   e) C & B
   f) None of the above

4) During the investigative phase, a knowledgeable forensics professional will ensure that the subject computer system is carefully handled to ensure that:
   a) no possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer.
   b) no computer viruses were introduced during the analysis phase.
   c) investgations are made directly on the affected system.
   d) A & C
   e) B &C
   f) A & B

5) What are three main steps of the Investigative Phase?
   a) Copy, examine, correct
   b) Identify, preserve, examine
   c) Identify, examine, assess
   d) Confiscate, Log, Correct

6) Every phase of the Incident Response Plan should be completed for every reports of an anomaly. True or **False**?

7) All employees must read and initial their understanding of the policies on overall computer security. **True** or False?

8) Every violation of a corporate security policy is an intentional, dishonest act. True or **False**?

9) All results of an investigation should be turned over to law enforcement for criminal prosecution or civil proceedings. True or **False**?

10) Once an attack has occurred, the company should then spend the time and money to develop an effective incident-handling plan. True of **False**.

Last Updated: July 25th, 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 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
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
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
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS