Sample Incident Cause Analysis Workflow

Table of Contents

Cause Analysis Example .................................................................................................................. 3
Cyber Incident Cause Analysis ........................................................................................................ 4
Initiating Problem, Event, or Threat Vector .................................................................................. 6
Deliberate Attack ........................................................................................................................... 7
Initial Foothold .............................................................................................................................. 9
Vulnerability/Exploit Code -1 ........................................................................................................ 10
Vulnerability/Exploit Code -2 ........................................................................................................ 11
Impersonation ............................................................................................................................... 12
Configuration/Feature Abuse ....................................................................................................... 13
Denied of Service .......................................................................................................................... 14
Authentication ............................................................................................................................... 15
Theft of Equipment ....................................................................................................................... 16
Other ............................................................................................................................................. 17
User Involvement .......................................................................................................................... 18
Privilege Escalation on Initial Foothold ......................................................................................... 19
After the Initial Foothold ............................................................................................................... 20
Spreading ...................................................................................................................................... 21
Privilege Escalation ....................................................................................................................... 23
Initiating Problem, Event, or Threat Vector .................................................................................. 24
Incident with No Attacker ............................................................................................................. 25
Policy Violations ............................................................................................................................ 26
Cause Analysis Example

The following slides show one possible root cause analysis model that categorizes incidents along these attack/threat vectors:

- deliberate attack
  - initial foothold
  - after the initial foothold
- incident with no attacker

This model is based on and expanded from the Microsoft Broad Street Taxonomy, which is focused on malware propagation methods.


**013 And this one's based on a taxonomy that Microsoft developed as part of their Broad Street project, and that particular Broad Street project was designed to identify malware propagation methods and identifying and categorizing how malicious code is propagated.

So we took some of those high-level characteristics from the Broad Street taxonomy, which looks at features and characteristics such as user interaction, whether or not there was a vulnerability exploited, and are there any configurable preventative measures that can be put in place, and expanded out to look beyond
just malware and look at other types of typical attacks and threats. And the higher level is looking at whether or not this was a deliberate attack by a malicious intruder, and distinguishing that from all the other types of innocents where there was no malicious attacker.

And then going down the tree of different possibilities, we'll look at other characteristics of each of these higher-level categories and we'll step through these in more detail.

**Cyber Incident Cause Analysis**

![Partial, high-level diagram of some possible threat vectors](image)

**014 So here's looking at a higher-level view of looking at a process**
workflow and comparing this—again, this is adapted from Microsoft's Broad Street taxonomy—but we're looking, first identifying if there is an attacker, and if there was not, then is there some other reason—explanation, some root cause—that allowed that particular incident to occur. Again, we're going to want to go back and look at a different catalog or a list of all different possibilities that could be used to explain any type of cause for a particular incident, and then include these in our overlying process taxonomy.

Generally for those incidents that there were an attacker, we'll want to identify things as how they initially gained access to the resources that are used. Did they have any user interaction or involvement to allow them access, or they exploit vulnerabilities? Once they got into the system, were they able to escalate their privileges and were they able to spread or propagate that access to other types of systems? So for each of these questions that we're trying to identify yes or no if we can, based on the available data resources, there are follow-up questions that we'll want to address until we can get a complete picture of the underlying causes and what happened in that particular incident.
Initiating Problem, Event, or Threat Vector

Was the incident due to a deliberate attack?

Deliberate attacks
- deliberately stolen equipment
- an employee clicking a bad link from an email
- an employee connecting an already infected laptop to the employer’s network
- insiders deliberately harming the organization
- an incident involving malicious code

Incidents with no attacker
- lost equipment
- an employee accidentally sending email to the wrong person or list and divulging sensitive information
- an employee accidentally failing to encrypt PII
- an employee accidentally taking data home that should not leave the facility
- other internal problems that were not initiated by a ruse, fraudulent information, or coercion

**015 So we'll step through each of the different high levels on these coming slides, and so-- this is identifying whether or not it was a deliberate attack versus an incident that was inadvertent or accidental-- so distinguishing between an attack where someone actually stole a laptop or a piece of equipment versus a use who accidentally lost accidentally lost a piece of equipment or a device. Different patterns and different follow-up approaches and investigations we're going to pursue depending on the answers to these questions.
An employee might have been tricked and they clicked on a link or they downloaded some malicious code, or maybe the intruder exploited some kind of vulnerability-- a variety of different things distinguishing deliberate attacks from inadvertent or accidental incidents.

**Deliberate Attack**

If the incident included a deliberate attack, try to identify two types of information:

1. The **initial attack** that allowed the attacker to gain a foothold into the organizational infrastructure
   - cause of the “initial foothold”
   - user involvement during attainment of initial foothold
   - privilege escalation on initial foothold

2. Any spreading, propagation, or follow-on incidents **after the initial attack** (initial foothold gained)
   - spreading
   - privilege escalation

**016** If it was a deliberate attack, some of the things that we’re going to want to try to identify is, after the initial attack occurred, what was the underlying cause to allow them to gain that unauthorized access. Was there any kind of user involved in the initiation of that initial foothold, and were they able
to escalate their privileges? Maybe they were able to get a user account or information or password and then later on, one they got access to a system, they were able to exploit some other local vulnerability to gain higher levels of privileges after that initial foothold into the system.

And the second path that we're going to want to pursue is after that initial foothold of the attack, was there further spreading of their access, if they were using malware, or were they able to escalate privileges later on as part of their course of actions?
**Initial Foothold**

**Was the attacker able to establish an initial foothold?**

If yes, then try to identify the initial threat vector:

- vulnerability/exploit code
  - how it was delivered
  - CVE name of the vulnerability
  - vulnerable software that was targeted by the exploit
- impersonation
- configuration/feature abuse
- denial of service
- authentication
- theft of equipment

**017 So some of the specific details looking at the initial foothold. Can we identify was there any kind of vulnerability that was exploited, and if so, what do we know about that vulnerability? Is there some identifying characteristics--a CVE name, do we have some idea of how it was delivered? If it was a zero day vulnerability and we don’t know, was there some other mechanism that was used instead of or in addition to that?**

Perhaps they were taking advantage of some configuration or feature, or abusing some inherent characteristics of the system. For certain types of
incidents, maybe a denial of service was involved. Perhaps they were taking advantage of poor authentication mechanisms or they were stealing equipment or other data to allow them to get that initial foothold. So enumerating the different types of possibilities of how an intruder might have been able to cause an incident and they identifying which of those various causes might have been used in this particular instance.

Vulnerability/Exploit Code -1

Vulnerability/Exploit Code -1

If the initial foothold was the result of an attack that involved remote exploit code (e.g., malicious attachment, web link), try to identify information about the vulnerability that was exploited and how the exploit was delivered.

How was the exploit delivered?

• web browser
• email
• web (non-browser)
• agency-run/provided application, service, or site
• media
• hardware

**018 After the initial foothold was gained, if a vulnerability was being exploited, can you identify how that
exploit was delivered? Typical

types of examples might be through

e-mail, vulnerabilities in different

applications like web browsers, or

there's other applications that might

have unpatched vulnerabilities-- a

variety of different ways to exploit

software vulnerabilities and

identifying the method used is going
to be useful.

**Vulnerability/Exploit Code -2**

**Vulnerability/Exploit Code -2**

What details are known about the vulnerability?

- Common Vulnerabilities and Exposures (CVE) name of the

vulnerability

- vulnerable software that was targeted by the exploit

- version of the targeted software, including patches, updates,

  hotfixes, etc.

- exploit command, code, or exploit that was run

  and/or what that code injected

- sites, domain names, addresses, or other servers involved

- available traffic to/from affected systems

**019 In addition, if it's a

known vulnerability, cataloging and

identifying any specific

characteristics-- the CVE name, the

particular software that was

vulnerable to that particular
vulnerability, if there was any
particular exploit tool or command or
script that was used that's well
known-- just basically kind of a mini
vulnerability analysis, as much
information that's available.

**Impersonation**

**Impersonation**

**Did the attacker pretend to be another party?**

Classic examples of impersonation attacks are those that trick
users into divulging information or installing a piece of software.
(Generally, these attacks are not combined with a vulnerability or
exploit.)

Other examples include
• an email or online form asking a user to provide his or her
  username and password
• pop-up ads that claim to install legitimate software but instead
  install malware such as fake antivirus or other software

**020** If impersonation was used--
in other words, the attacker tried to
pretend to be someone else--
in a phishing email or something else,
trying to get the user to click on a
link or follow something that might
allow some vulnerable or malicious
code to be exploited, trying to
identify some of these answers.
Configuration/Feature Abuse

Was the initial foothold obtained as the result of an attack that was able to abuse features or weak configurations?

If yes, try to identify the

• local environment and its settings
• details of the configuration before delivery
• how the threat was initially delivered
• subsequent changes that resulted from delivery, such as file reads/writes
• behavior that executed the feature abuse and indicators (files modified, path writes attempted, etc.) that the behavior occurred

examples: misuse of Autorun, such as for propagation of malicious files, Office macros, or file-infecting viruses

**021 Examples of configuration or feature abuse were taking advantage of weak environmental settings in the local system; there may be some information as to how the initial reconfiguration was exploited or were there actual changes made to configurations after the initial foothold was gained, such as adding additional files, changing registry settings and things like that. And these are just some examples of various types of known configuration or feature weaknesses on systems.
Was a denial of service involved?

(A denial of service is also referred to as attrition in the Microsoft Broad Street taxonomy.)

If yes, then try to identify

- how the brute force method was delivered
- details such as the originating source system(s) and the traffic it sent
- the system(s) targeted by the brute force and any other pertinent information on the traffic involved in the attack

examples: denial of service (DoS), telephony denial of service (TDoS), distributed denial of service (DDoS), or other instances where brute force methods are used (with the exception of attacks against passwords, logins, sessions, or other authentication mechanisms)

**022 If there was a denial-of-service attack involved, then try to identify how it was delivered. Was it different styles, different types, brute force, just overwhelming system resources with traffic, distinguishing between a simple denial-of-service attack versus maybe a more complex distributed denial-of-service attack, or other types of denial of services, whether the target of the attack in this particular incident.
Authentication

**Authentication**

**Was the initial foothold caused by an authorized account being used by an unauthorized person?**

If yes, try to identify the

- account used (privileged or non-privileged, expired, default)
- type of authentication used to log in (password, hardware token, biometrics)
- the technical indicators used to determine that the user was not authorized

examples: repeated login attempts, session brute force, password brute force, stolen credentials, guessed credentials

**023 If there are reasons that allow the intruder to bypass authentication mechanisms, try to identify what was used, what particular accounts-- was it a user-level account versus a privileged, administrator or root-level account? Did they use simple, reusable passwords, or were there other types of multifactor authentication that might have been exploited or taken advantage of? Is there any other kind of information that can identify whether or not the authentication allowed unauthorized access to other types of accounts? And a variety of different ways to compromise authentication methods by cracking**
passwords or sniffing passwords or just merely guessing them if the passwords are weak enough.

Theft of Equipment

**Theft of Equipment**

Was equipment stolen?
If yes, identify the stolen equipment (e.g., badges, media, devices, laptops).

**024 The other category, if equipment was stolen versus just being lost-- and depending on what the equipment was, if it was a laptop or other-- maybe a USB drive or removable media or even a CD-- maybe there was information on that particular equipment or on the data or even an access badge that could allow physical access to a system, this could be another factor in identifying how the incident occurred.
Other

**Was another threat vector involved?**

If the initial foothold was the result of some other threat, try to identify

- what happened
- how it was initially delivered

**025 Then there might be some case where there might be some other unidentified or it's unknown or you don't have access to the information to conclusively identify if it was any of the other common types of vulnerabilities or weaknesses or threat vectors that allowed an intruder to get that initial foothold.**
User Involvement

Did attaining the initial foothold involve the actions of one or more users?

Was it partially caused by the actions of users?

Try to identify whether the

- user was not involved
- user was deceived
  - The user was deceived, and the attack used an exploit.
  - The user was deceived without using an exploit.
- user was not deceived

**026 Another path to pursue, as we mentioned, is whether or not users were involved. Many times the users are the weak link in allowing an intruder initial access, but if they weren’t, then identifying those were the incident occurred without any user interaction. But for those that did involve user action, try to identify whether or not the user was deceived of if they weren’t, and typical ways that they might be deceived was using an exploit or without an exploit.
Did privilege escalation occur on the initial foothold?
If yes, try to identify the mechanism used to perform privilege escalation:

- vulnerability/exploit code
- impersonation
- configuration/feature abuse
- authentication
- other

* Escalation is explained in more detail in later slides.

**027 So they may be just linked to a phishing website, or maybe there is an attachment to a message and they opened that attachment and installed that particular malicious code.

After the initial foothold was gained, if privilege escalation occurred, try to identify how that privilege escalation occurred, whether it was through exploiting a vulnerability, using impersonation, or some of the other things we talked about-- configuration weaknesses or authentication weaknesses-- and it may be some other type of weakness that allowed privilege escalation to
occur that’s not one of these more common types.

**After the Initial Foothold**

**After the Initial Foothold**

Did the attack expand beyond the initial foothold and spread to other assets in the organization?

- spreading
- privilege escalation

*028 And then after the initial foothold was gained, identifying how much the access spread and if there was further later privilege escalation beyond that initial foothold.*
Spreading

Did the attack spread to other machines or network assets after the initial foothold was established?

If yes, try to identify the following:

• How did the attack continue to spread?
  - vulnerability/exploit code
  - impersonation
  - configuration/feature abuse
  - denial of service
  - authentication
  - theft of equipment
  - other

• How persistent was the spreading?
  - survived past system restart
  - survived past commercial antivirus cleaning (with known signatures)
  - survived reinstallation of operating system
  - examples: TDL rootkit and BIOS infections

**029 So by spreading, we're looking at did this unauthorized access spread to other types of systems, other machines, other network assets, and if so, try to identify how that occurred. Was it by using the same kind of accounts, compromised accounts, impersonating those accounts, on other systems that had the same authentication passwords? Was it by exploiting other vulnerabilities or the same vulnerability on other systems? So we're going through some of the same questions but looking at the other systems that may be involved beyond this.
And then another factor of spreading is identifying how persistent was that spreading. Sometimes the spreading can be stopped simply by shutting down or restarting the system and it’ll flush any information that might be in memory. However, sometimes the spreading might persist past the initial restart of the system and it might even survive past things like trying to eradicate the initial code with commercial antivirus products. Or even after cleaning and recovering the system, rebuilding it from the original distribution media and patching it, there may still be techniques to regain access by installing certain types of library root kits or BIOS infections that would survive and give the intruder access beyond the initial cleaning or eradication mechanisms used.
Privilege Escalation

Did privilege escalation occur during the rest of the attack after the initial foothold was attained?

If yes, try to identify the following information:

- technique or method that attackers used to perform the privilege escalation
- description of the method used
- whether the method required users to be involved
- outcome of the privilege escalation (i.e., the result achieved)
- number of times the method was used
- whether the escalation was from one account to another one, or just an expansion of an existing account

**030 So some of the things that we're trying to identify in the privilege escalation portion: Whatever specific technique, if it's known, or be able to identify through looking at the available resources; describing what method was used to perform that privilege escalation and whether or not it involved users. What was the result achieved by escalating that privilege? Did they get root or administrator access? How often was it reused? And whether it was just using specific accounts or expanding the privileges from one account to others. So these are some of the various possibilities in privilege escalation attacks.**
Initiating Problem, Event, or Threat Vector

**Initiating Problem, Event, or Threat Vector**

**Was the incident due to a deliberate attack?**

**Deliberate attack**
- deliberately stolen equipment
- an employee clicking a bad link from an email
- an employee connecting an already infected laptop to the employer’s network
- insiders deliberately harming the organization
- any incident involving malicious code

**Incidents with no attacker**
- lost equipment
- an employee accidentally sending email to the wrong person or list and divulging sensitive information
- an employee accidentally failing to encrypt PII
- an employee accidentally taking data home that should not leave the facility
- other internal problems that were not initiated by a ruse, fraudulent information, or coercion

**031 So that goes through a variety of different common ways in trying to trace back and identify the various factors or features, root causes, if incidents that were deliberate, but then to have a full taxonomy, you also want to identify root causes for the incidents where there was no malicious attacker, as we mentioned earlier. Some examples were accidents, where employees or users inadvertently might not follow procedures and allow information to leak or spill from one system to another.**
Incident with No Attacker

Was the incident due to a deliberate attack?
If no, identify the other cause(s).
These incidents do not have an attacker or adversary attempting to manipulate users.

Causes
• natural disaster
• physical accident
  - internal
  - external
• system failure
• equipment loss
• policy violation

**032 So these are some other examples of where there are no deliberate attacks. It could be physical accidents. Internal or external accidents could cause a denial of service if there's a severed cable outside of your facilities and you're no longer connected to the internet. It could be other types of system failures or equipment losses or other types of policy violations that were deliberate, but these are various underlying root causes that might be applicable to different types of incidents that don't involve an attacker.
Policy Violations

If the cause of the incident was due to a violation of security policies (affecting the confidentiality, integrity, or availability of information or information systems), identify the sub-category.

Policy violation causes include

• data security
• unauthorized software installed
• unauthorized hardware/device installed
• improperly configured device
• shared credentials

**033 Examples of some of the policy violations might include data security policies; policies, as we mentioned, prohibiting unauthorized installation of software or hardware or other devices to be connected to your network; perhaps just poorly or weakly configured devices or people sharing their passwords or credentials with other users.
Data Security Policy Violations

If the cause of the incident was due to a data security policy violation (e.g., improper/insufficient access control), identify the sub-category.

Data security policy violation causes include

- improper information disclosure
  - improperly stored information
  - improperly marked information
  - improperly transferred information
- improper information modification
- improper information destruction
- denial of service

**034 Other features to look for in looking at data security policy violations-- if it was a violation, trying to identify what the impact of that was. Was it information that was improperly disclosed, and if so, was it disclosed during the storage or the transfer or just improper marking of the information? Or was the information just unauthorized, modified or deleted? Perhaps it wasn't leaked out, but there was unauthorized changes or the loss of data that may have been not deliberate and just could have been caused by an accident.
Example – Putting It into Practice

Incident scenario: a website was defaced with a hacktivist message.

Let’s do a root cause analysis on this incident:

- Was the incident due to a deliberate attack?
- Was the attacker able to establish an initial foothold?
- Did the initial foothold involve actions of one or more users?
- Did the attack spread to other systems or networks?
- Did privilege escalation occur?

**035 So an example of putting this root cause analysis method, process into place in a particular incident. Here we look at a typical type of incident where we have a website and it was discovered to be defaced and an attacker put a hacktivist message on the home landing page. So trying to put this particular scenario through our root cause analysis using the previous method, we’d look at the questions: Was it a deliberate attack? If so, were they able to establish an initial foothold? Did it involve any user interaction? Did it spread to other systems or networks? And was there any privilege escalation that occurred?
Was the incident due to a deliberate attack?
− Yes
• Was the attacker able to establish an initial foothold?
  − Yes: exploited known vulnerability in web server
• Did the initial foothold involve actions of one or more users?
  − No
• Did the attack spread to other systems or networks?
  − No
• Did privilege escalation occur?
  − Yes: replaced home page with defaced web page

**036 So for this particular scenario, was it deliberate? Well yes, it does appear to be, and because of the message that was put there, this didn't occur by accident. And how was the attacker able to establish an initial foothold? If you have the data sources and can identify it, you might identify that this particular web server had an unpatched vulnerability. This was a known vulnerability but a patch hadn't been applied in time, so the intruder exploited this vulnerability. An alternate scenario: Maybe it was unknown or zero day vulnerability. So the answer to these questions and some of the other follow-up details might be known.
Next question: Did they gain an initial foothold involving user interaction? By looking at the available resources, we might be able to identify that no, no user interaction was involved. By exploiting this vulnerability remotely, they were able to gain that initial access. Did the attack spread to other systems or networks? In this case, the answer appears to be no. It's just this one web server that was involved.

And did privilege escalation occur? Well, in this case, depending on how you define privilege escalation, they were able to replace the homepage, modify data, files, on the system with an alternate page. So yes, they were able to get privileges of the web server, whoever owned that particular webpage, to make the changes on the web server. So looking in a little bit more detail--
Example – Root Cause Analysis -2

How do you identify/verify (confirm or refute) that a particular threat vector or root cause was responsible for the incident?

- Was the attacker able to establish an initial foothold?
  - Yes: exploited known vulnerability in web server

Possible scenario – using the results of other analysis steps

- Log file analysis leads to detection of unknown files (artifacts) on the victim system.
- Artifact analysis of files includes the generation of MD5 checksums.
- Comparison of MD5 checksums against malware catalog identifies a file as malware that exploits a known vulnerability.
- Analysis of the victim system shows that it was running an unpatched, vulnerable version of the software exploited by the detected malware.
- Further analysis of system log files confirms the symptoms reported by the analyzed malware catalog (e.g., antivirus was disabled, hidden processes were running, command and control data was transmitted with external systems).

**037 How do you verify that the particular root cause was responsible? So looking at the issue, we’re able to identify that the known vulnerability was exploited in the web server.

Looking at other results in the analysis steps, some of the things you might want to look at are looking at the log files on that particular web server and see if you can find any artifacts or other remnants of what the intruder did on that particular web server. Looking at the analysis of the files might identify that there was a new file, and looking at the checksums of those, you may be able to identify and look up from other
external resources, such as malicious code or other malware catalogs, that this particular MD5 checksum for this file matches an exploit that does indeed exploit a known vulnerability. So that can lead you to identifying which vulnerability was exploited and confirming that this vulnerability had somehow gone unpatched.

Further analysis of this web server shows that it was running that particular version of the vulnerable software that was used by this particular malware exploit, and then further analysis of looking at the system logs on the web server confirms some of the systems that had been identified in the analyzed malware from the other sources. Typical symptoms for this piece of malware would be that it would disable its antivirus, it would hide processes that were running, and it would also set up a command-and-control structure with other external systems from that web server. So knowing this would give you some further course of action and things to look for to further analyze and identify what other systems may have been involved, if it was indeed this same exploit that was used to gain foothold into this web server.

So that's just one example of how you might apply a formalized series of questions to come up with a root cause analysis method or process and applying that to a cybersecurity incident.
**So here's just a pictorial diagram looking at- a very simplified view in this scenario. Yes, we did have an attacker. They gained initial foothold by exploiting a known vulnerability. There was no user involvement or spreader propagation in this particular case, but they were able to get privileges equivalent to that of whoever owned that webpage to replace the homepage with their message and exploiting that vulnerability on the particular systems.**
Copyright 2016 Carnegie Mellon University

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon®, CERT® and CERT Coordination Center® are registered marks of Carnegie Mellon University.

DM-0003588