


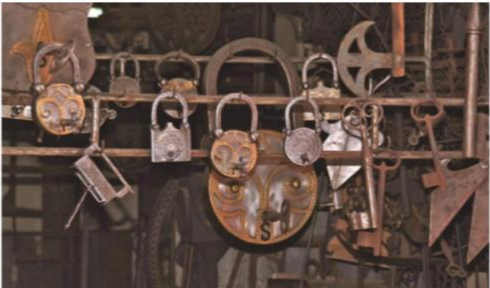
Incident Response: Foundations of Incident Response

Slide 1



Principles of Computer Security, Fifth Edition


Incident Response



Foundations of Incident
Response

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we discuss the foundations of incident response.



Principles of Computer Security, Fifth Edition


Foundations of Incident Response

- **Incident** – any event in an information system or network where the behavior is different than normal.
- **Incident response** – the steps an organization performs in response to an incident.
- IR involves the entire business
 - Security team at center
- Many causes; Results sorted by impact
- Need guidelines for determining level of response.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

An **incident** is any event in an information system or network where the behavior is different than normal. **Incident response** is a term used to describe the steps an organization performs in response to any situation determined to be abnormal in the operation of a computer system. Incident response is not just an information security operation; it is an effort that involves the entire business. The security team may form a nucleus of the effort, but the key tasks are performed by many parts of the business. There are many ways for an incident to occur. The environment, attackers, and user error are probably general enough to capture most causes. The primary concern of incident response, however, is not why, but what. That is, the cause of the incident is not the first concern, but rather the impact and determining how to respond. A low-impact incident may not result in any significant risk exposure, so no action other than repairing the broken system is needed. A moderate-risk incident will require greater scrutiny and response effort.

A high-level risk exposure incident will require the greatest scrutiny and response effort. To better manage incidents when they occur, some guidelines need to be created to assist the incident response team in determining the level of response required. In other words, how to triage an incident.




Principles of Computer Security, Fifth Edition

Foundations of Incident Response

- Two major elements for determining level of response.
 - **Information criticality** – the relative importance of specific information to the business.
 - Comes from data classification and quantity
 - Affect on business operations.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Two major elements play a role in determining the level of response. Information criticality is the primary determinant, and this comes from the data classification and the quantity of data involved. **Information criticality** is the relative importance of specific information to the business. Information criticality is a key measure used in the prioritization of actions throughout the incident response process. The loss of one administrator password is less serious than the loss of all of them. The second major element involves a business decision on how this incident affects current business operations. A series of breaches, whether minor or not, indicates a pattern that can have public relations and regulatory consequences.



Principles of Computer Security, Fifth Edition

Foundations of Incident Response


- Incident □ Response
- Incident Response Plan
 - Solid, well-rehearsed
 - Custom-tailored to the information criticalities, hardware and software architectures, and people.
- Challenges rapidly become organizational in nature: budget, manpower, resources, and commitment.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Once an incident happens, it is time to react with a solid, well-rehearsed incident response plan.

This plan is custom-tailored to the information criticalities, the actual hardware and software architectures, and the people.

Like all large, complex projects, the challenges rapidly become organizational in nature—budget, manpower, resources, and commitment.



Principles of Computer Security, Fifth Edition

Incident Management


- Incident Response Management is a key risk mitigation strategy.
- Establish a CIRT/CERT
 - **Computer Incident Response Team (CIRT)**
 - **Computer Emergency Response Team (CERT)**
- Incident □ CIRT investigates and makes recommendations
- CIRT membership should be diverse and flexible and determined *before* an incident

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Having an incident response management methodology is a key risk mitigation strategy.

One of the steps that should be taken to establish a plan to handle business interruptions as a result of a cyber event of some sort is the establishment of a **Computer Incident Response Team (CIRT)** or a **Computer Emergency Response Team (CERT)**. They're both pronounced "sert" and which is which is not typically an important distinction. One distinction is that incident response covers all incidents whereas emergency response typically only covers incidents which are emergencies. Another distinction is that the CERT name is trademarked by the SEI at CMU and so is only used by permission from the CERT coordination center.

When an incident occurs, the organization's **CIRT** will conduct the investigation into the incident and make the recommendations on how to proceed. The CIRT should consist of not only permanent members but also ad hoc members who may be called upon to address special needs depending on the nature of the incident. In addition to individuals with a technical background, the CIRT should include nontechnical personnel to provide guidance on ways to handle media attention, legal issues that may arise, and management issues regarding the continued operation of the organization. The CIRT should be created and team members should be identified before an incident occurs. Policies and procedures for conducting an investigation should also be worked out in advance of an incident occurring. It is also advisable to have the team periodically meet to review these procedures.



Principles of Computer Security, Fifth Edition

Goals of Incident Response

- Confirm or dispel incident
- Promote accurate information accumulation and dissemination
- Establish controls for evidence
- Protect privacy rights
- Minimize disruption to operations
- Allow for legal/civil recourse
- Provide accurate reports/recommendations

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Incident response depends upon accurate information.

Without it, the chance of following data in the wrong direction is a possibility, as is missing crucial information and only finding dead ends.


These goals are essential for the efficacy of an incident response process.

Incident response depends upon accurate information.

Without it, the chance of following data in the wrong direction is a possibility, as is missing crucial information and only finding dead ends.

These goals are essential for the efficacy of an incident response process.

Incident response depends upon accurate information. Without it, the chance of following data in the wrong direction is a possibility, as is missing crucial information and only finding dead ends. These goals are essential for the efficacy of an incident response process. Confirm or dispel reports of the incident Promote accurate information accumulation and dissemination Establish and enforce controls for evidence Protect privacy rights Minimize disruption to operations Allow for legal or civil recourse And provide accurate reports and recommendations.




Principles of Computer Security, Fifth Edition

Anatomy of an Attack

- Attackers have a method by which they attack a system.
 - Specifics may differ from event to event.
 - Common steps employed
- Two ends of the attack spectrum
 - Old School
 - APTs

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Although the specifics of an attack may differ from event to event, there are some steps that are commonly employed. There are numerous types of attacks, from old-school hacking to the new advanced persistent threats. The differences are subtle and are related to the objectives of each form of attack.



Principles of Computer Security, Fifth Edition

Old School

1. Footprinting – define boundaries
2. Scanning – reconnaissance
3. Enumeration – list systems and make plan
4. Gain Access – get in
5. Escalate Privilege – get root
6. Pilfer – steal information
7. Create Backdoors – enable easy reentry
8. Cover Tracks – erase logs
9. Denial of Service – deny access

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Attacks are not a new phenomenon in enterprise security, and an examination of attacks throughout history show some common methods.

The traditional steps of an old school attack include footprinting, scanning, enumeration, gain access, escalate privilege, pilfer, create backdoors, cover tracks, and denial of service (DOS).


Footprinting is the determination of the boundaries of a target space. There are numerous sources of information, including web sites, DNS records, and IP address registrations. Understanding the boundaries assists an attacker in knowing what is in their target range and what isn't. Scanning is the examination of machines to determine what operating systems, services, and vulnerabilities exist. The enumeration step is a listing of the systems and vulnerabilities to build an attack game plan.

The first actual incursion is the gaining of access to an account on the system, almost always an ordinary user, as higher-privilege accounts are harder to target.

The next step is to gain access to a higher-privilege account by escalating privileges.

From a higher-privilege account, the range of accessible activities is greater, including pilfering files, creating back doors so you can return, and covering you tracks by erasing logs.

The detail associated with each step may vary from hack to hack, but in most cases, these steps were employed in this manner to achieve an objective.



Principles of Computer Security, Fifth Edition

Advanced Persistent Threat

1. Define target – e.g. footprinting
2. Research target – scanning, open-source intelligence
3. Select tools – e.g. enumeration, custom malware, etc.
4. Test for detection – dry run
5. Initial intrusion – go phishing
6. Establish outbound connection – phone home
7. Obtain credentials – get access
8. Expand access – get more access
9. Strengthen foothold – get deeper and more diverse access
10. Cover tracks – tamper with logs
11. Exfiltrate data – steal information

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A relatively new attack phenomenon has been labeled the **advanced persistent threat**.

An **advanced persistent threat (APT)** is an attack that always maintains a primary focus on remaining in the network, operating undetected, and having multiple ways in and out.

APTs began with nation-state attackers, but the utility of the long-term attack has proven valuable, and many sophisticated attacks have moved to this route.

The attack methodology is similar to the traditional old-school attack method, but additional emphasis is placed on the steps needed to maintain a presence on a network:

An attack typically begins with a research and reconnaissance phase where the attacker determines what to attack and how.

For the actual intrusion, most APTs begin with social engineering, such as phishing, to establish a foothold in the system under attack.

Custom malware use makes detection of the attack by antivirus/malware programs a near impossibility.

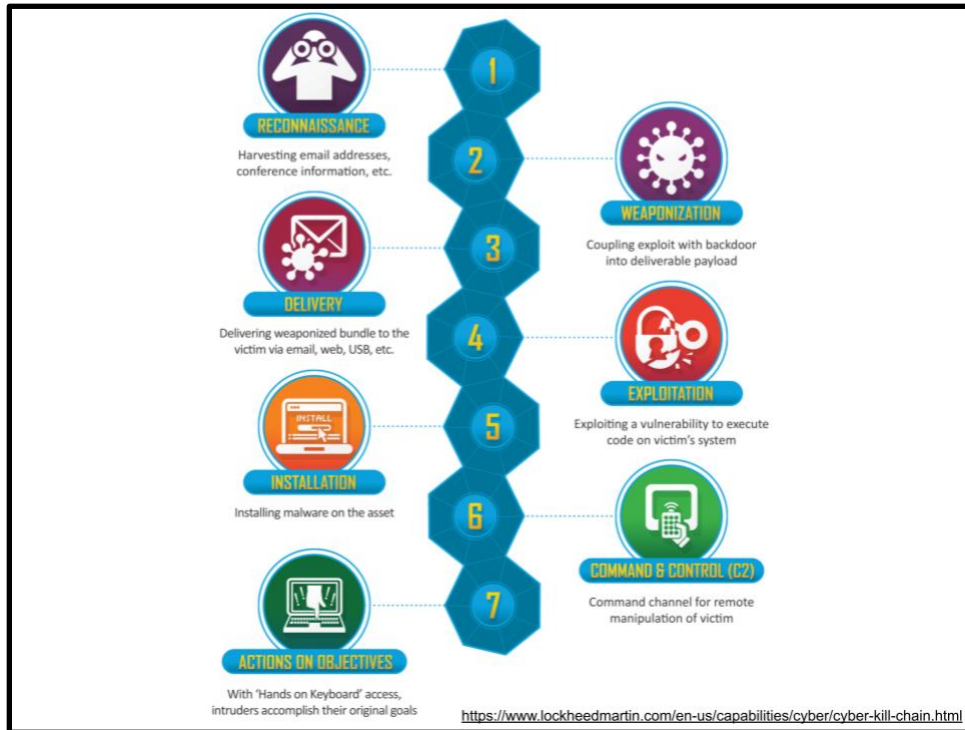
Once initial access is obtained, tools like **remote administration trojans** are planted in the victim's network, creating network backdoors and tunnels allowing stealth access to its infrastructure.

The next step, obtaining credentials and escalating privileges, is performed through the use of exploits and password cracking. The goal is to get as much access as possible, and to have hooks into the system as deep as possible.


One of the hallmarks of an APT attack is the emphasis on maintaining a presence on the system to ensure continued control over access channels and credentials acquired in previous steps.

A common technique for expanding access is lateral movement across a network, obtaining access and control of servers, workstations, and other connected devices. Attackers also perform internal reconnaissance to learn more about the system, the organization, and the people. Eventually, the APT will gain access to information worth having and will proceed to exfiltrate it in some stealthy way.

Slide 10



A modern cyberattack is a complex, multistage process. The concept of a kill chain is the targeting of specific steps of a multistep process with the goal of disrupting the overall process. The term **cyber kill chain** is the application of the kill chain philosophy to a cyber incident, with the expressed purpose of disrupting the attack. The **Cyber Kill Chain®** framework was developed by Lockheed Martin. This figure comes from their website and shows 7 steps of an attack. The earlier you can stop the attacker on this chain, the better. The chain also helps to identify layers of defenses that can be employed to make reaching the end of the chain as hard as possible.




Principles of Computer Security, Fifth Edition

Threat Intelligence

- Actionable information about malicious actors, their tools, infrastructure, and methods.
- Cannot protect everything against all threats
- Where to apply incident response resources in response to an incident?
- Threat Intelligence + cyber kill chain = prioritization of actions

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Threat intelligence is the actionable information about malicious actors, their tools, infrastructure, and methods. No firm has the resources to protect everything against all threats or investigate all possible hostile actions. Thus, a critical decision is where to apply incident response resources in response to an incident. A combination of threat intelligence combined with the concept of the kill chain (the attacker's most likely path) gives you some means to prioritize actions against the most meaningful threats.



Principles of Computer Security, Fifth Edition

Attribution


- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.


Incident Response: Incident Response Process

Slide 1



Principles of Computer Security, Fifth Edition


Incident Response



Incident Response Process

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we begin our discussion of the incident response process.




Principles of Computer Security, Fifth Edition

Incident Response Process

- Incident response is the set of actions security personnel perform in response to a wide range of triggering events.
 - These actions are vast and varied because they have to deal with a wide range of causes and consequences.
 - Through the use of a structured framework, coupled with properly prepared processes, incident response becomes a manageable task.
 - Without proper preparation, this task can quickly become impossible or intractably expensive.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Incident response is the set of actions security personnel perform in response to a wide range of triggering events. These actions are vast and varied because they have to deal with a wide range of causes and consequences. Through the use of a structured framework, coupled with properly prepared processes, incident response becomes a manageable task. Without proper preparation, this task can quickly become intractable or impossible.



Principles of Computer Security, Fifth Edition

Incident Response Process

- Incident response is the new business cultural norm in information security.
- Incident response is a multistep process with several component elements.
 - The first is organization preparation, followed by system preparation.
 - An initial detection is followed by initial response, then isolation, investigation, recovery, and reporting.
 - There are additional process steps of follow-up and lessons learned.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Incident response is the new business cultural norm in information security.

The key is to design the procedures to include appropriate business personnel, not keep it as a pure information security endeavor.


The challenges are many, including the aspect of timing as the activities quickly become a case of one group of professionals pursuing another.

Incident response is a multistep process with several component elements.

The first is organization preparation, followed by system preparation.

An initial detection is followed by initial response, then isolation, investigation, recovery, and reporting.

Finally, there are the additional process steps of follow-up and lessons learned.



Principles of Computer Security, Fifth Edition


Incident Response Process

- Incident response is a key element of a security posture and must involve many different aspects of the business to properly respond.
- This is best built upon the foundation of a comprehensive **incident response policy** that details the roles and responsibilities of the organizational elements with respect to the elements of the process.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Incident response is a key element of a security posture and must involve many different aspects of the business to properly respond.

This is best built upon the foundation of a comprehensive **incident response policy** that details the roles and responsibilities of the organizational elements with respect to the elements of the process.




Principles of Computer Security, Fifth Edition

Preparation

- **Preparation** for an incident is the first phase.
- The organization needs to:
 - Establish the steps to be taken when an incident is discovered (or suspected)
 - Determine points of contact
 - Train all employees and security professionals so they understand the steps to take and who to call
 - Establish an incident response team
 - Acquire the equipment and train those who will use the equipment

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Incident response efforts begin before an incident occurs—that is, before “something goes wrong.” During the preparation phase, the organization needs to Establish the steps to be taken when an incident is discovered (or suspected) Determine points of contact Train all employees and security professionals so they understand the steps to take and who to call Establish an incident response team and acquire the equipment and train those who will use the equipment.



Principles of Computer Security, Fifth Edition


Organization Preparation

- Develop and maintain comprehensive incident response policies and procedures
- Establish and maintain an Incident Response Team
- Obtain top-level management support
 - Agree to ground rules/rules of engagement
 - Develop scenarios and responses
- Develop and maintain an incident response toolkit
 - System plans and diagrams
 - Network architectures
 - Critical asset lists
- Practice response procedures
 - Fire drills
 - Scenarios (“Who do you call?”)

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Organization preparation requires a plan, both for the initial effort and for maintenance of that effort. Over time, the organization shifts based on business objectives, personnel change, business efforts and focus change, new programs, new capabilities; virtually any change can necessitate shifts in the incident response activities. At a minimum, the following items should be addressed and periodically reviewed in terms of incident response preparation:

- Develop and maintain comprehensive incident response policies and procedures
- Establish and maintain an Incident Response Team
- Get the support of top-level management, which includes agreeing to rules of engagement and developing scenarios and responses
- Develop and maintain an incident response toolkit, which includes system plans and diagrams, network architectures, and lists of critical assets
- Practice response procedures such as fire drills and scenarios.



Principles of Computer Security, Fifth Edition

System Preparation

- Systems require preparation for effective incident response efforts.
- Incident responders depend on documentation to understanding hardware, software, and network layouts.
- A common incident response question: “who can do what?”
 - Requires understanding access control across all systems.
- Incident response data retrieval
 - Made easier by understanding the logging methodology and architecture.
- System investigation
 - Made more efficient by lists of critical files and integrity checks

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


Systems require preparation for effective incident response efforts. Incident responders are dependent upon documentation for understanding hardware, software, and network layouts. Understanding how access control is employed, including specifics across all systems, is key when determining who can do what.

Understanding the logging methodology and architecture will make incident response data retrieval easier. Having lists of critical files and their hash values, all stored offline, can make system investigation a more efficient process. All of these questions should be addressed in the design and implementation of diagrams, access control, and logging, to ensure that these critical security elements are capturing the correct information before an incident.

In the end, when architecting a system, taking the time to plan for incident response processes will be crucial to a successful response once an incident occurs.

Preparing systems for incident response is similar to preparing them for maintainability, so these efforts can yield regular dividends to the system owners.

Determining the steps to isolate specific machines and services can be a complex endeavor, and is best accomplished during the preparation phase before an incident.



Principles of Computer Security, Fifth Edition

Researching vulnerabilities

- Researching vulnerabilities should occur prior to an attack.
- Information on vulnerabilities in specific application programs and operating systems:
 - <https://nvd.nist.gov/>
 - <https://cve.mitre.org/cve/>
- Red team / Blue team
 - Red: role play as attacker
 - Blue: defender


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

After the hacker has a list of software running on the systems, they will start researching the Internet for vulnerabilities associated with that software.

Numerous web sites provide information on vulnerabilities in specific application programs and operating systems.

Understanding how hackers navigate systems is important. System administrators and security personnel can use the same steps to research potential vulnerabilities before a hacker strikes.

This information is valuable to administrators who need to know what problems exist and how to patch them.



Principles of Computer Security, Fifth Edition

Incident Response Team

- Establishing an incident response team is an essential step in the preparation phase.
- Incident Response Team – group of people that prepares for and responds to any emergency incident, such as a natural disaster or an interruption of business operations.
- Members are highly skilled and diverse
- Critical part of IR plan

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


The complete handling of an incident typically takes an entire team.

Establishing an incident response team is an essential step in the preparation phase.

An incident response team is a group of people that prepares for and responds to any emergency incident, such as a natural disaster or an interruption of business operations.

A computer security incident response team in an organization typically includes members who bring a wide range of skills to bear in the response effort.

Incident response teams are common in corporations as well as in public service organizations and are a critical part of the incident response plan.



Principles of Computer Security, Fifth Edition

Incident Response Team

- IR team members trained to fulfill the roles required by the specific situation.
- Dynamically sized to the scale and nature of an incident.
- Advanced preparation of relationships with higher-level groups is important.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


Incident response team members ideally are trained and prepared to fulfill the roles required by the specific situation (for example, to serve as incident commander in the event of a large-scale public emergency).

Incident response teams are frequently dynamically sized to the scale and nature of an incident, and as the size of an incident grows and as more resources are drawn into the event, the command of the situation may shift through several phases.

In a small-scale event, or in the case of a small firm, usually only a volunteer or ad hoc team may exist to respond.

In cases where the incident spreads beyond the local control of the incident response team, higher-level resources through industry groups and government groups exist to assist in the incident.

Advanced preparation in the form of contacting and establishing working relations with higher-level groups is an important preparation step.



Principles of Computer Security, Fifth Edition

Incident Response Team Membership

- Team lead
- Network/security analyst
- Internal and external subject matter experts
 - e.g. HW, SW, Forensics, business
- Legal counsel
- Public affairs officer
- Security office contact
- Law enforcement liaison

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


In determining the specific makeup of the team for a specific incident, there are some general points to think about. The team needs a leader, preferably a higher-level manager who has the ability to obtain cooperation from employees as needed. It also needs a computer or network security analyst, since the assumption is that the team will be responding to a computer security incident.

Specialists may be added to the team for specific hardware or software platforms as needed. It may be an IT system being investigated, but the data, processes, and value all belong to the business, and the business is the element that understands the risk and value of what is under attack.

Having key, knowledgeable business members on the incident response team is a necessity to ensure that the security actions remain aligned with the business goals and objectives of the organization. The organization's legal counsel should be part of the team on at least a part-time or as-needed basis. The public affairs office should also be available on an as-needed basis, because it is responsible for formulating the public response should a security incident become public.

The organization's security office should also be kept informed. It should designate a point of contact for the team in case criminal activity is suspected, in which case, care must be taken to preserve evidence should the organization decide to push for prosecution of the individual(s).

There is no one size fits all response team membership checklist. How the team is composed depends on the organization. In any case, the who, what, and when of team formation needs to be specified in the incident response policy during the preparation phase.



Principles of Computer Security, Fifth Edition

Attribution


- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.


Incident Response: Incident Response Process Pt. 2

Slide 1



Principles of Computer Security, Fifth Edition


Incident Response



Incident Response Process
Part 2

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we continue our discussion of the incident response process.




Principles of Computer Security, Fifth Edition

Incident Response Plan

- An **incident response plan** is documentation associated with the steps an organization performs in response to any situation determined to be abnormal in the operation of a computer system.
- Two major elements play a role in determining the level of response.
 - Information criticality is the primary determinant
 - The second factor involves a business decision on how this incident plays into current business operations.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

An **incident response plan** is documentation associated with the steps an organization performs in response to any situation determined to be abnormal in the operation of a computer system. Two major elements play a role in determining the level of response. Information criticality is the primary determinant. The second factor involves a business decision on how this incident plays into current business operations.



Principles of Computer Security, Fifth Edition

Documented incident types/category definitions

- Provide planners and responders with a set number of preplanned scripts.
- Example categories
 - Interruption of service
 - Malicious communication
 - Data exfiltration
 - Malware delivery
 - Phishing attack

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Documented incident types/category definitions provide planners and responders with a set number of preplanned scripts that can be applied quickly, minimizing repetitive approvals and process flows.

Example categories are:

Interruption of service

Malicious communication


Data exfiltration

Malware delivery

Phishing attack

And so on

This list should be customized to meet the IT needs of the organization.



Principles of Computer Security, Fifth Edition


Roles and responsibilities

- Must define the roles and responsibilities of the incident response team members.
- Roles and responsibilities may vary slightly based on the identified categories.
- Defining them before an incident occurs empowers the team to perform the necessary tasks.
 - Cut connections, change servers, start/stop services

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

It is very important to define the roles and responsibilities of the incident response team members.

The defined roles and responsibilities may vary slightly based on the identified categories, but defining them before an incident occurs empowers the team to perform the necessary tasks during the time-sensitive aspects of an incident.




Principles of Computer Security, Fifth Edition

Reporting requirements/escalation

- Planning the desired **reporting requirements** including escalation steps is an important part of the operational plan for an incident.
 - Who will talk about the incident and to whom?
 - How does information flow?
 - Who needs to be involved?
 - When should the issue be escalated to higher levels?
- Questions are best handled in the calm of a pre-incident planning meeting where the procedures are created rather than on the fly as an incident is occurring.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Planning the desired **reporting requirements** including escalation steps is an important part of the operational plan for an incident. Questions are best handled in the calm of a pre-incident planning meeting where the procedures are created rather than on the fly as an incident is occurring.



Principles of Computer Security, Fifth Edition


Cyber-incident response teams

- Defining the cyber-incident response team, including identifying key membership and backup members, is a task that needs to be done prior to an incident occurring.
- The planning aspect of incident response needs to define who is on the team, whether a dedicated team or a group of situational volunteers, and what their duties are.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Defining the cyber-incident response team, including identifying key membership and backup members, is a task that needs to be done prior to an incident occurring.

The planning aspect of incident response needs to define who is on the team, whether they are a dedicated team or a group of situational volunteers, and what their duties are.




Principles of Computer Security, Fifth Edition

Exercise

- No plan survives contact with the enemy
- **Exercises** come in many forms and functions.
- Doing a tabletop exercise where planning and preparation steps are tested is an important final step.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

You don't really know how well a plan will work until it is tested. **Exercises** come in many forms and functions and doing a tabletop exercise where planning and preparation steps are explicitly tested is an important final step.



Principles of Computer Security, Fifth Edition

Incident Identification/Detection

- An **incident** is defined as a situation that departs from normal, routine operations.
 - 1st determination: important or not?
- A suspected incident must first be detected.
 - IR team: actual security incident?
 - IR team investigates. Treat as security incident by default.
 - Security incidents can take a variety of forms.
 - Virus or social engineering,
 - Reporting procedure needs to be in place.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

An **incident** is defined as a situation that departs from normal, routine operations.

Whether an incident is important or not is the first determination to be made as part of an incident response process. A single failed login is technically an incident, but if it is followed by a correct login, then it is not of any consequence. In fact, this could even be considered as normal. But 10,000 failed attempts on a system, or failures across a large number of accounts, are distinctly different and may be worthy of further investigation.

Many things can be misinterpreted as a possible security incident. For example, a software bug in an application may cause a user to lose a file, and the user may blame this on a virus or similar malicious software.

The incident response team must investigate each reported incident and treat it as a potential security incident until it can determine whether it is or isn't. This means that your organization will want to respond initially with a limited response team before wasting a lot of time having the full team respond. This is the initial step to take when a report is received that a possible incident has been detected.

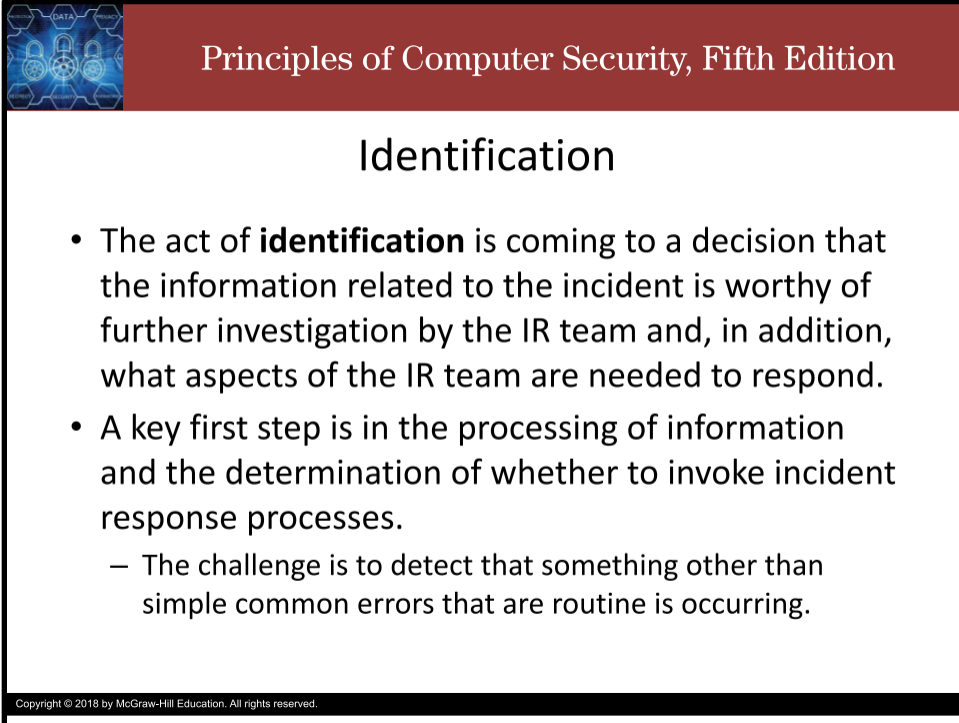
Security incidents can take a variety of forms, and who discovers the incident will vary as well. One of the groups most likely to discover an incident is the team of network and security administrators who run devices such as the organization's firewalls and intrusion detection systems.

Another common incident is a virus. Several packages are available that can help an organization detect potential virus activity or other malicious code. Administrators will often be the ones to notice something is amiss, but so might an average user who has been hit by the virus.

Social engineering is a common technique used by potential intruders to acquire information that may be useful in gaining access to computer systems, networks, or the physical facilities that house them. Anybody in the organization can be the target of a social engineering attack, so all employees need to know what to be looking for regarding this type of attack. In fact, the target might not even be one of your organization's employees—it could be a contractor, such as somebody on the custodial staff or nighttime security staff.

Whatever the type of security incident suspected, and no matter who suspects it, a reporting procedure needs to be in place for the employees to use when an incident is detected. Everybody needs to know who to call should they suspect something, and everybody needs to know what to do. A common technique is to develop a reporting template that can be supplied to an individual who suspects an incident, so that the necessary information is gathered in a timely manner.

Slide 9



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. To the left of the header is a small graphic of a blue hexagonal grid with various icons. The main content area is white with a black border. The title "Identification" is centered in a large, bold, black font. Below the title is a bulleted list with three items. The first item is a bullet point followed by a paragraph. The second item is a bullet point followed by a paragraph. The third item is a bullet point followed by a paragraph with a sub-bullet point. At the bottom left of the slide, there is a small copyright notice.

Principles of Computer Security, Fifth Edition

Identification

- The act of **identification** is coming to a decision that the information related to the incident is worthy of further investigation by the IR team and, in addition, what aspects of the IR team are needed to respond.
- A key first step is in the processing of information and the determination of whether to invoke incident response processes.
 - The challenge is to detect that something other than simple common errors that are routine is occurring.

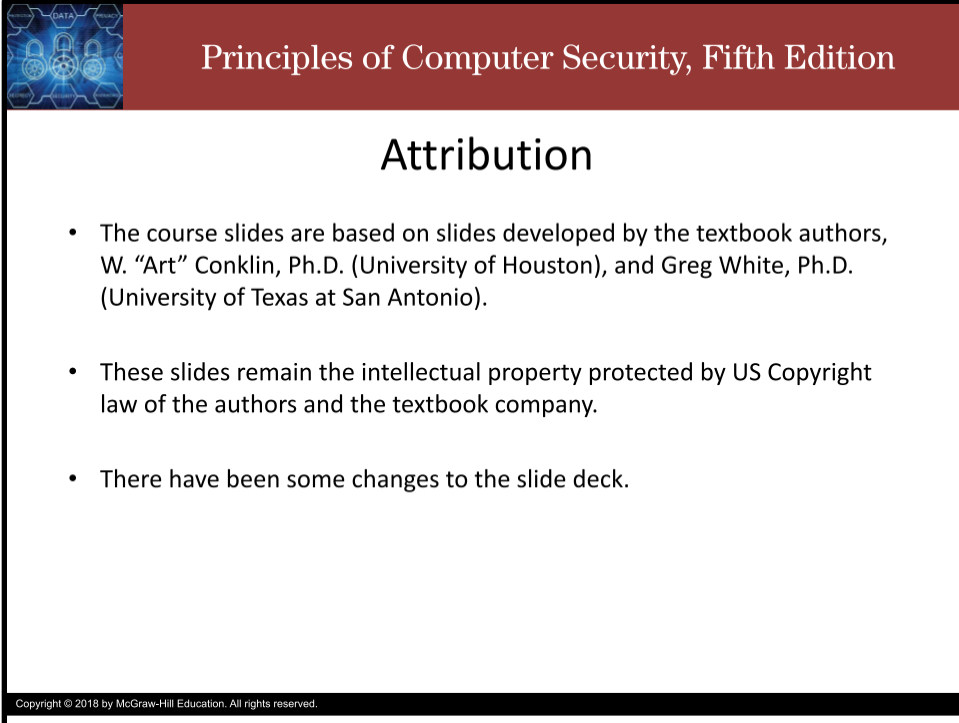
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The act of **identification** is coming to a decision that the information related to the incident is worthy of further investigation by the IR team and, in addition, what aspects of the IR team are needed to respond.

A key first step is in the processing of information and the determination of whether or not to invoke incident response processes.

Incident information can come from a wide range of sources, including logs, employees, help desk calls, system monitoring, security devices, and more. The challenge is to detect that something other than simple common, routine errors is occurring. When evidence accumulates, or in some cases when specific items such as security device logs indicate a potential incident, the next step is to escalate the situation to the incident response team.

Slide 10



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. To the left of the header is a small graphic of blue padlocks and gears. The main content area is white with a black border. The title "Attribution" is centered in a large, bold, black font. Below the title is a bulleted list of three items. At the bottom left of the slide, there is a small copyright notice.

Principles of Computer Security, Fifth Edition

Attribution


- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.


Incident Response: Incident Response Process Pt. 3

Slide 1



Principles of Computer Security, Fifth Edition


Incident Response



Incident Response Process
Part 3

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we continue our discussion of the incident response process.



Principles of Computer Security, Fifth Edition

Initial Response


- The following items are important to determine during an **initial response**:
 - Current time and date
 - Who/what is reporting the incident
 - Nature of the incident
 - When the incident occurred
 - Hardware/software involved
 - Point of contact for involved personnel

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Although there is no such thing as a typical incident, for any incident there is a series of questions that can be answered to form a proper initial response

Regardless of the source, it is important to determine the following bits of information during an **initial response**:

- The current time and date
- Who/what is reporting the incident
- The nature of the incident
- When the incident occurred
- The hardware or software involved
- A point of contact for involved personnel.



Principles of Computer Security, Fifth Edition

Initial Response


- The following items are important to determine during an **initial response**:
 - Current time and date
 - Who/what is reporting the incident
 - Nature of the incident
 - When the incident occurred
 - Hardware/software involved
 - Point of contact for involved personnel

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The purpose of an initial response is to begin the incident response action and place it on a proper pathway toward success.

The initial response must support the goals of the information security program. If something is very critical, treating it as routine would be a mistake, so triage with respect to information criticality is important. The initial response must also be aligned with the business practices and objectives. Triage with respect to current business imperatives and conditions is important. The initial response actions need to be designed to comply with administrative and legal policies as well as to support decisions with regard to civil, administrative, or criminal investigations/actions. For these purposes, maintaining a forensically sound process from the beginning is important.

It is also important that the information is delivered accurately and expeditiously to the appropriate decision-makers so that future actions can be timely. One of the greatest tools to achieve all of these goals is a simple and efficient process, so establishing fewer steps that are clear and clean is preferred. Complexity in the initial response process only leads to issues later because of delays, confusion, and incomplete information.



Principles of Computer Security, Fifth Edition

Cyber First Responder

- A cyber first responder must do as much as possible to control damage or loss of evidence.
 - As time passes, evidence can be tampered with or destroyed.
 - The first responder can do much to prevent damage, or can cause significant loss by digitally altering evidence, even inadvertently.
 - Collecting data should be done in a forensically sound way, and be sure to pay attention to recording time values so time offsets can be calculated.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


A cyber first responder must do as much as possible to control damage or loss of evidence.

As time passes, evidence can be tampered with or destroyed.

- Look around on the desk, on the Rolodex, under the keyboard, in desktop storage areas, and on cubicle bulletin boards for any information that might be relevant.
- Secure floppy disks, optical discs, flash memory cards, USB drives, tapes, and other removable media.
- Request copies of logs as soon as possible. Most ISPs will protect logs that could be subpoenaed.
- Take photos (some localities require use of instant-developing photos like a Polaroid camera, as they are more difficult to modify without obvious tampering) or video.
- Include photos of operating computer screens and hardware components from multiple angles. Be sure to photograph internal components before removing them for analysis.

The first responder can do much to prevent damage, or can cause significant loss by digitally altering evidence, even inadvertently.

Collecting data should be done in a forensically sound way, and be sure to pay attention to recording time values so time offsets can be calculated.




Principles of Computer Security, Fifth Edition

Containment/Incident Isolation

- Once an incident is discovered and characterized, the most important step in the incident response process involves the isolation of the problem.
 - Many incidents can spread to other machines and expand the damage footprint if not contained.
 - When a particular machine or service becomes compromised, the team can invoke the preplanned steps to isolate the infected unit from others.
 - This may have an impact on performance, but it will still be less than if the compromise is allowed to spread and more machines become compromised.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Once an incident is discovered and characterized, the most important step in the incident response process involves the isolation of the problem. Many incidents can spread to other machines and expand the damage footprint if not contained. When a particular machine or service becomes compromised, the team can invoke the preplanned steps to isolate the infected unit from others. This may have an impact on performance, but it will still be less than if the compromise is allowed to spread and more machines become compromised.



Principles of Computer Security, Fifth Edition

Containment and eradication are next steps


- Once the incident response team has determined that an incident most likely has occurred, it must attempt to quickly contain the problem.
- At this point, or very soon after containment begins, depending on the severity of the incident, management needs to decide whether the organization intends to prosecute the individual who has caused the incident or simply wants to restore operations as quickly as possible without regard to possibly destroying evidence.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The next steps are **Containment** and eradication.

Once the incident response team has determined that an incident most likely has occurred, it must attempt to quickly contain the problem.

At this point, or very soon after containment begins, depending on the severity of the incident, management needs to decide whether the organization intends to prosecute the individual who has caused the incident or simply wants to restore operations as quickly as possible without regard to possibly destroying evidence.



Principles of Computer Security, Fifth Edition


Decide how to address containment

- Stay connected and attempt to determine the origin of the intruder.
- Disconnect from the Internet until the system can be restored and vulnerabilities can be patched.
- Add filtering rules or modifying existing rules on firewalls, routers, and intrusion detection systems, updating antivirus software, and removing specific pieces of hardware or halting specific software applications.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The incident response team must decide how to address containment as soon as it has determined that an actual incident has occurred. If the attacker is still connected, one option is to stay connected and attempt to determine the origin of the intruder.

Or, never mind the attacker, just panic disconnect from the Internet until the system can be restored and vulnerabilities can be patched. Other containment options include adding filtering rules or modifying existing rules on firewalls, routers, and intrusion detection systems, updating antivirus software, and removing specific pieces of hardware or halting specific software applications.



Principles of Computer Security, Fifth Edition


The Cause of the Incident

- Once the immediate problems have been contained, the incident response team needs to address the cause of the incident.
 - Vulnerability patch it
 - Compromised account lock it
 - Insider attack terminate them
 - Intern mistake roast them
- Determining when an intruder first gained access to your system or network is critical in determining how far back to go in restoring the system or network.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Once the immediate problems have been contained, the incident response team needs to address the cause of the incident.

Determining when an intruder first gained access to your system or network is critical in determining how far back to go in restoring the system or network.



Principles of Computer Security, Fifth Edition

Quarantine

- One method of isolating a machine is through a quarantine process.
 - **Quarantine** is a process of isolating an object from its surroundings, preventing normal access methods.
 - Quarantine can be accomplished through a variety of mechanisms, including the erection of firewalls restricting communication between machines.
 - This can be complex process but if properly configured in advance, quarantine operation limitations can allow the machine to continue to run for diagnostic purposes.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


One method of isolating a machine is through a quarantine process.

Quarantine means isolating an object from its surroundings, preventing normal access methods.

The machine may be allowed to run, but its connection to other machines is broken in a manner to prevent the spread of infection.

Quarantine can be accomplished through a variety of mechanisms, including the erection of firewalls restricting communication between machines.

This can be complex process but if properly configured in advance, the limitations of the quarantine operation limitations can allow the machine to continue to run for diagnostic purposes.



Principles of Computer Security, Fifth Edition

Device Removal

- In the event that a machine becomes compromised, it is simply removed from production and replaced.
- When device removal entails the physical change of hardware, this is a resource-intensive operation.
- The reimaging of a machine can be a time-consuming and difficult endeavor.
- The advent of virtual machines changes this entirely, as the provisioning of virtual images on hardware can be accomplished in a much quicker fashion.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


Device removal is a more extreme response.

In the event that a machine becomes compromised, it is simply removed from the production environment and replaced with a clean machine.

When device removal entails the physical change of hardware, this can be a resource-intensive operation.

The reimaging of a machine can also be a time-consuming and difficult endeavor.

However, the advent of virtual machines changes this entirely, as the provisioning of virtual images on hardware can be accomplished in a much quicker fashion.



Principles of Computer Security, Fifth Edition

Escalation and Notification

- One key decision point in initial response is that of escalation.
 - When a threshold of information becomes known to an operator and the operator decides to escalate the situation, the incident response process moves to a notification and escalation phase.
 - Incident response efforts should map to the actual risk level associated with the incident.
 - When the incident response team is notified of a potential incident, its first steps are to confirm the existence, scope, and magnitude of the event and then respond accordingly.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


One key decision point in initial response is that of escalation.

When a threshold of information becomes known to an operator and the operator decides to escalate the situation, the incident response process moves to a notification and escalation phase. Not all incidents have the same risk profile and incident response efforts should be scaled to match the actual risk level associated with the incident.

When the incident response team is notified of a potential incident, its first steps are to confirm the existence, scope, and magnitude of the event and then respond accordingly.

Making an assessment of the risk associated with an incident is an important first step. If the characteristics of an incident include a large number of packets destined for different services on a machine (an attack commonly referred to as a port scan), then the actions needed are different than those needed to respond to a large number of packets destined to a single machine service. Port scans are common, and to a degree relatively harmless, but port flooding can result in denial of service.

Making a determination of the specific downstream risks is important in prioritizing response actions.



Principles of Computer Security, Fifth Edition

Strategy Formulation

- How critical are the impacted systems?
- How sensitive is the data?
- What is the potential overall dollar loss involved/rate of loss?
- How much downtime can be tolerated?
- Who are the perpetrators?
- What is the skill level of the attacker?
- Does the incident have adverse publicity potential?


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The response to an incident will be highly dependent upon the particular circumstances of the intrusion. There are many paths one can take in the steps associated with an incident. The challenge is choosing the best steps in each case. During the preparation stage, a wide range of scenarios can be examined, allowing time to formulate strategies. Even after an incident response team has planned a series of strategies to respond to various scenarios, determining how to employ those preplanned strategies to proper effect still depends on the circumstances of a particular incident.

A variety of factors should be considered in the planning and deployment of strategies, such as:

- How critical are the impacted systems?
- How sensitive is the data?
- What is the potential overall dollar loss involved/rate of loss?
- How much downtime can be tolerated?
- Who are the perpetrators?
- What is the skill level of the attacker?
- Does the incident have adverse publicity potential?

These pieces of information provide boundaries for the upcoming investigations.



Principles of Computer Security, Fifth Edition

Strategy Formulation

- Addressing these issues helps provide focal points during the investigation
 - Restore normal operations
 - Determine public relations play
 - Determine probable attacker
 - Determine type of attack
 - Classify victim system

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There are still numerous issues that need to be determined with respect to the upcoming investigation. Addressing these issues helps provide focal points during the investigation.

How should we restore normal operations? Offline recovery? Or Online recovery?


What's our public relations play? "To spin or not to spin?", that is the question. Whether tis nobler in the press to suffer the slings and arrows of righteous anger, or to take arms against a sea of critics and by fibbing distract them...

Who attacked us? Do we involve law enforcement? No. Don't talk to the police. If the attacker was internal: do we handle the matter internally or do we push for prosecution? If they were external: do we prosecute? Do we hack them back?

What kind of attack was it? DoS, theft, vandalism, policy violation? Is it still an ongoing intrusion? Did they pivot once they got in? Where to?

What kind of system did they attack? A critical server/application? How many users? What other systems are affected?

Using the answers to these questions helps the team determine the necessary steps in the upcoming investigation phase. Although it is impossible to account for all circumstances, this level of strategy can greatly assist in scoping the work ahead during the investigation phase.



Principles of Computer Security, Fifth Edition

Attribution


- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.


Incident Response: Incident Response Process Pt. 4

Slide 1



Principles of Computer Security, Fifth Edition


Incident Response



Incident Response Process
Part 4

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we conclude our discussion of the incident response process.



Principles of Computer Security, Fifth Edition

Investigation

- The investigation phase of an incident is a multistep, multiparty event.
 - With the exception of very simple events, most incidents will involve multiple machines and potentially impact the business in multiple ways.
- The primary objective of the investigative phase is to make the following determinations:
 - What happened
 - What systems are affected
 - What was compromised
 - What was the vulnerability
 - Who did it (if possible to determine)
 - What are the recovery/remediation options

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The investigation phase of an incident is a multistep, multiparty event.


With the exception of very simple events, most incidents will involve multiple machines and potentially impact the business in multiple ways.

The primary objective of the investigative phase is to make the following determinations:

- What happened?
- What systems are affected?
- What was compromised?
- What was the vulnerability?
- Who did it (if possible to determine)?
- What are the recovery/remediation options?

Looking at the list, it is daunting, but this is where the real work of incident response occurs.

It will take a team effort, partly because of workload, partly because of specialized skills, and partly because the entire effort is being performed in a race against time.



Principles of Computer Security, Fifth Edition

Duplication


- Duplication of drives is a common forensic process.
 - It is important to have accurate copies and proper hash values so that any analysis is performed under proper conditions.
 - Proper disk duplication is necessary to ensure all data, including metadata, is properly captured and analyzed as part of the overall process.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Duplication of drives is a common forensic process.

It is important to have accurate copies and proper hash values so that any analysis is performed under proper conditions.

Proper disk duplication is necessary to ensure all data, including metadata, is properly captured and analyzed as part of the overall process.




Principles of Computer Security, Fifth Edition

Network Monitoring

- To monitor network flow data, including who is talking to whom, one source of information is traffic analysis.
 - NetFlow is Cisco's protocol/standard for the collection of network metadata on the flows of network traffic.
 - Others: sFlow, Jflow, AppFlow, Cflowd
 - IPFIX (based on NetFlow v9) is now an IETF standard, and allows for unidirectional captures of communication metadata.
 - Traffic analysis can identify both common and unique data flows
 - new and unique patterns are of most interest to incident responders.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

To monitor network flow data, including who is talking to whom, one source of information is traffic analysis data. NetFlow is a protocol/standard for the collection of network metadata on the flows of network traffic. IPFIX (which is based on Cisco NetFlow version 9) is now an IETF standard, and allows for unidirectional captures of communication metadata. Traffic analysis can identify both common and unique data flows, and in the case of incident response, typically the new and unique patterns are of most interest to incident responders.




Principles of Computer Security, Fifth Edition

Eradication

- Removing the problem may mean rebuilding a clean machine.
- Prevention of reinfection is key.
- VMs give the ability to rebuild quickly.
 - makes eradication relatively easy.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Once a problem has been contained to a set footprint, the next step is eradication. **Eradication** involves removing the problem, and in today's complex system environment, this may mean rebuilding a clean machine. A key part of operational eradication is the prevention of reinfection. Presumably, the system that existed before the problem occurred would be prone to a repeat infection, and thus reinfection needs to be specifically guarded against. One of the strongest value propositions for virtual machines is the ability to rebuild quickly, making the eradication step relatively easy.



Principles of Computer Security, Fifth Edition


Recovery

- Returning an asset to normal business operations.
- **Recovery** is an important step in all incidents.
- One of the first rules is to not trust a system that has been compromised, and this includes all aspects of an operating system.
- Whether there is known destruction or not, the safe path is one where the recovery step includes reconstruction of affected machines.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Once the issue has been eradicated, the recovery process begins. Recovery means returning assets back to normal business operations. After eradication, the system is still isolated. The recovery process includes the steps necessary for returning the system to operational status.

Recovery is an important step in all incidents. One of the first rules is to not trust a system that has been compromised, and this includes all aspects of an operating system. Whether there is known destruction or not, the safe path is one where the recovery step includes reconstruction of affected machines.



Principles of Computer Security, Fifth Edition

Recovery

- Recovery efforts involve several specific elements.
 - Identify and resolve cause of incident.
 - Examine affected data and what to do about it
- Recovery can be a two-step process.
 - Recover essential business functions.
 - Complete restoration of services and operations.
- Restoration can be done in a wide variety of ways.
- A key aspect in many incidents is that of external communications. (forthright and honest PR)

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Recovery efforts involve several specific elements:

First, the cause of the incident needs to be determined and resolved.

Second, the data, if sensitive and subject to misuse, needs to be examined in the context of how it was lost, who would have access, and what business measures need to be taken to mitigate specific business damage as a result of the release.


Recovery can be a two-step process.

First, the essential business functions can be recovered, enabling business operations to resume.

The second step is the complete restoration of all services and operations

Restoration can be done in a wide variety of ways. Sometimes, reinstalling a clean operating system is sufficient. Sometimes only a few files and applications need to be replaced. Other times the firmware needs to be reflashed and all the storage media replaced, at which point it may just be cheaper to buy a whole new machine. But simply swapping out with a new machine is not sufficient. If they got you once, they can get you again. The new machine needs to be protected against reinfection.

A key aspect in many incidents is that of external communications. How the incident is handled by the organization and the public's perception thereof are often the most influential factors in determining the final cost of the incident.



Principles of Computer Security, Fifth Edition

Reporting

- After the system has been restored, the incident response team creates a report of the incident.
 - The report acts as a corporate memory and can be used for future incidents.
 - The report allow a mechanism to close the loop with management over the incident.
 - The report provides a roadmap of the actions that can be used in the future to prevent events of identical or similar nature.
 - Part of the report will be recommendations.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


After the system has been restored, the incident response team creates a report of the incident.

Detailing what was discovered, how it was discovered, what was done, and the results, this report acts as a corporate memory and can be used for future incidents. Having a knowledge base of previous incidents and the actions used is a valuable resource because it is in the context of the particular enterprise.

These reports also allow a mechanism to close the loop with management over the incident and, most importantly, provide a roadmap of the actions that can be used in the future to prevent events of identical or similar nature.

Part of the report will be recommendations, if appropriate, to change existing policies and procedures, including disaster recovery and business continuity.

The similarity in objectives makes a natural overlap, and the cross-pollination between these operations is important to make all processes as efficient as possible.




Principles of Computer Security, Fifth Edition

Lessons Learned

- Important to collect **lessons learned** and assign action items to correct weaknesses
- A few last items
 - Senior-level management must be informed about what occurred and what was done to address it.
 - An after-action report should be created to outline what happened and how it was addressed.
 - If prosecution of the individual responsible is desired, additional time will be spent helping law enforcement agencies and possibly testifying in court.
 - Training material may need to be developed or modified.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

In the reporting process, a critical assessment of what went right, what went wrong, what can be improved, and what should be continued is prepared as a form of **lessons learned**. This is a critical part of self-improvement, and is not meant to place blame, but rather to assist in future prevention. Having things go wrong in a complex environment is part of normal operations; having repeat failures that are preventable is not. The key to the lessons learned section of the report is to make the necessary changes so that a repeat event will not occur. Because many incidents are a result of attackers using known methods, once the attack patterns are known in an enterprise and methods exist to mitigate them, then it is the task of the entire enterprise to take the necessary actions to mitigate future events.



Principles of Computer Security, Fifth Edition

Attribution


- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.


Incident Response: Standards and Best Practices

Slide 1



Principles of Computer Security, Fifth Edition


Incident Response



Standards and Best Practices

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we discuss standards and best practices for incident response.




Principles of Computer Security, Fifth Edition

Standards and Best Practices

- There are many options available to a team when planning and performing processes and procedures.
- To assist the team in choosing a path, there are both standards and best practices to consult in the proper development of processes.
- From government sources to industry sources, there are many opportunities to gather ideas and methods, even from fellow firms.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There are many options available to a team when planning and performing processes and procedures. To assist the team in choosing a path, there are both standards and best practices to consult in the proper development of processes. From government sources to industry sources, there are many opportunities to gather ideas and methods, even from fellow firms.



Principles of Computer Security, Fifth Edition

State of Compromise

- The new standard of information security involves living in a state of compromise, where one should always expect that adversaries are active in their networks.
 - It is unrealistic to expect that you can keep attackers out of your network.
 - Operating in a state of compromise does not mean that one must suffer significant losses.
 - A working assumption is that the systems are compromised and that prevention cannot be the only means of defense.


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The new standard of information security involves living in a state of compromise, where one should always expect that adversaries are active in their networks.

It is unrealistic to expect that you can keep attackers out of your network.

Operating in a state of compromise does not mean that one must suffer significant losses.

A working assumption when planning for, responding to, and managing the overall incident response process is that the systems are compromised and that prevention cannot be the only means of defense.




Principles of Computer Security, Fifth Edition

NIST

- NIST has Special Publications in Computer Security
- SP 800 Series
 - Computer Security Incident Handling Guide, SP 800-61 Rev. 2
 - NIST Security Content Automation Protocol (SCAP), SP 800-126 Rev 2
 - Information Security Continuous Monitoring for Federal Information Systems and Organizations, SP 800-137
 - Guide to Selecting Information Technology Security Products, NIST SP 800-36
 - Guide to Enterprise Patch Management Technologies, NIST SP 800-40 Version 3
 - Guide to Using Vulnerability Naming Schemes [CVE/CCE], NIST SP 800-51 Rev 1

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The National Institutes of Standards and Technology (NIST), a U.S. governmental entity under the Department of Commerce, produces a wide range of Special Publications (SPs) in the area of computer security. Grouped in several different categories, the most relevant SPs for incident response come from the Special Publications 800 series. They are not very exciting reads, but they are the definitive guides for compliance in computer and network security. An entire career can be made out of being an expert on a particular SP.



Principles of Computer Security, Fifth Edition

Department of Justice

- The U.S. Department of Justice's Cybersecurity Unit released a best practices document:
 - [*Best Practices for Victim Response and Reporting of Cyber Incidents*](#)
- This document identifies:
 - Steps to take before a cyber incident
 - Steps to take during an incident response action
 - A list of actions to not take
 - What to do after the incident

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The U.S. Department of Justice's Cybersecurity Unit released in 2015 and revised in 2018 a best practices document titled [*Best Practices for Victim Response and Reporting of Cyber Incidents*](#)


This document identifies:

Steps to take before a cyber incident

Steps to take during an incident response action

A list of actions to not take

And What to do after the incident



Principles of Computer Security, Fifth Edition

Indicators of Compromise (IOCs)

- Artifacts left behind from computer intrusion activity.
 - Detection of IOCs is a quick way to jumpstart a response element.
 - IOCs have spread in usage to a wide range of firms.
 - IOCs act as a tripwire for responders.
 - An IOC can be tied to a specific observable event, which then can be traced to related events, and to stateful events such as Registry keys.
 - IOCs provide a means of getting on the trail of attackers.


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Incident response depends upon accurate information. Without it, the chance of following data in the wrong direction is a possibility, as is missing crucial information and only finding dead ends. These goals are essential for the efficacy of an incident response process.

Incident response depends upon accurate information. Without it, the chance of following data in the wrong direction is a possibility, as is missing crucial information and only finding dead ends. These goals are essential for the efficacy of an incident response process.

Indicators of Compromise (IOCs) are artifacts left behind from computer intrusion activity. Detecting IOCs is a quick way to jumpstart a response element. After being developed by Mandiant, IOCs have spread in usage to a wide range of firms. IOCs act as a tripwire for responders.

An IOC can be tied to a specific observable event, which then can be traced to related events, and to stateful events such as Registry keys. IOCs provide a means of getting on the trail of attackers, which can be one of the biggest challenges in incident response.



Principles of Computer Security, Fifth Edition

Indicators of Compromise

- [Structured Threat Information Expression \(STIX™\)](#) – a free and open source language and serialization format used to exchange cyber threat intelligence
- [OpenIOC](#) – an open source initiative established by Mandiant that is designed to facilitate rapid communication of specific threat information associated with known threats. [Redline](#) is free and uses OpenIOC.
- [Incident Object Description Exchange Format \(IODEF\)](#) – a data format which is used to describe computer security information for the purpose of exchange between Computer Security Incident Response Teams.


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Three of the main standards associated with IOCs are STIX, OpenIOC and IODEF.

[Structured Threat Information Expression \(STIX™\)](#) is a free and open source language and serialization format used to exchange cyber threat intelligence. MITRE's Cyber Observable eXpression (CybOX™) language, which is a structured language for cyber observables, has been integrated into STIX 2.0.

[OpenIOC](#) is an open source initiative established by Mandiant that is designed to facilitate rapid communication of specific threat information associated with known threats. FireEye, which acquired Mandiant in 2013, makes their [Redline](#) security software, which uses OpenIOC for triage, free to use.

[Incident Object Description Exchange Format \(IODEF\)](#) is a data format which is used to describe computer security information for the purpose of exchange between Computer Security Incident Response Teams.



Principles of Computer Security, Fifth Edition

Data Minimization

- Data requires protection in storage, in transit, and during processing.
 - The level of risk differs due to: time, quantity and access.
- **Data Minimization: Don't keep what you don't need.**
 - Minimization efforts begin before data even hits a system
 - During system design, the appropriate security controls are determined and deployed, with periodic audits to ensure compliance.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Data requires protection in each of the three states of the data lifecycle: in storage, in transit, and during processing. The level of risk in each state differs due to several factors: time, quantity and access.


All data in storage is subject to breach or compromise, and especially so since data spends most of its life in storage and a lot of data gets stored. A natural question is: what is the best mitigation strategy?

One primary mitigation step is **data minimization**. Data minimization efforts can play a key role in both operational efficiency and security.

One of the first rules associated with data is this: Don't keep what you don't need. This is least privilege applied to data.

Minimization efforts begin before data even hits a system, let alone a breach.

During system design, the appropriate security controls are determined and deployed, with periodic audits to ensure compliance.



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.