GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

End Users:
Assets or Liabilities When Handling a Cyber Incident?

Daniel Husmann

GIAC Security Essential Certification (GSEC)
Version 1.4b
Option 1
24 May 2004

© SANS Institute 2004, Author retains all rights.

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

TABLE OF CONTENTS Page
ABSTRACT 1
BACKGROUND 1
Phases of Incident Handling Process (Figure 1) 1
Preparedness 1
Identification 1
Containment 2
Eradication 2
Recovery 2
Lessons Learned 2
Another Approach 2
WACIRC Inbound Communications Framework (Figure 2) 3
BEFORE AN INCIDENT 3
Recognizing Computer Security Incidents 3
Social Engineering 4
People Making Mistakes 5
Financial Impacts of Security Breaches 6
Physical Security 6
Security and Acceptable Use Policies 7
DURING AN INCIDENT 7
Unnecessary Delays 7
Timely Reporting and Response 7
Opening the Door for Slammer (Figure 3) 8
Overloading Valuable Security Resources 9
Common Incident Types and Symptoms 9
Patch Management 9
AFTER AN INCIDENT 10
Recording and Documenting 10
Impact Assessment 10
Post Incident Review 11
Lessons Learned 11
Applying Lessons Learned to Policies and Procedures 11
Growth of Security Responsibility 12
WHAT CAN BE DONE TO IMPROVE THIS SITUATION? 12
HOW DO YOU EDUCATE END USERS ON SECURITY? 13
What Can Be Done BEFORE a Computer Security Incident 13
By Organizations: 13
By End Users 13
What Can Be Done DURING a Computer Security Incident 14
By Organizations: 14
By End Users 14
What Can Be Done AFTER a Computer Security Incident 14
By Organizations: 14
By End Users 15
CONCLUSION 15
REFERENCES 16

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

SANS Institute 2004 As part of GIAC practical repository Author retains full rights.

ABSTRACT:
End users can be the greatest asset to a CSIRT (Computer Security Incident Response Team) team during the life of a computer security incident. They can also be the biggest liability. End users play a critical role in the computer security incident response process from the time before an incident is recognized, all the way through to the final resolution. Recognizing the value and risk of the end users is paramount to success of the CSIR Team in response to computer security exploits. Investing in the end user's security education compounds the value of the CSIR Team.

BACKGROUND
Handling of most computer security incidents follows a predictable path. As shown in the diagram below, there are six phases in the process of handling a computer security incident.

PHASES OF INCIDENT HANDLING PROCESS[1]

PREPAREDNESS
IDENTIFICATION
CONTAINMENT
ERADICATION
RECOVERY
LESSONS LEARNED

Figure 1. Phases of Incident Handling

Preparedness
In the SANS model for incident response above, you can see the Preparedness phase is where most organizations do security prevention.

Identification
The Identify phase is when the incident or potential incident is typically reported. At this point some action is taken to identify the cause and determine if it is an operational problem masquerading as a security incident or a valid security incident justifying a response from the CSIR Team. This is also the phase in which the incident is formally declared, after it has been identified.

© SANS Institute 2003, Author retains all rights.

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Containment
In the Containment phase security resources attempt to limit the damage and impact of the security incident, while they continue to isolate the cause. This is where the security resources are trying to arrest the security incident and stop it's propagation through your environment.

Eradication
In the Eradication phase security resources within your organization attempt to remove any existence of the incident and correct any abnormalities that may have developed due to the incident. This is where a clear understanding of the incident is necessary to ensure all the occurrences of the incident have been removed from your environment and any complications caused by the incident are also corrected.

Recovery
In the Recovery phase all affected security assets are being rebuilt, rebooted, restored, or recovered back to their state prior to the incident, or as close as possible to that. This is where resources are double checked against the known incident specifics to ensure there is no existence of the incident, or collateral damage from the incident. If there were consequences from the incident, they would be resolved in this phase.

Lessons Learned
In the Lessons Learned phase the organization attempts to analyze the details of the incident's initiation, infection, attack, or infiltration of your environment. By analyzing the incident, the organization can implement appropriate prevention mechanisms or processes to eliminate the chance of re-infection or to mitigate the damage, should it occur again.

Another Approach
In simpler terms, there are 3 major phases of a computer security incident, BEFORE an incident occurs, DURING the time when the incident is active in your environment, and AFTER the incident has been closed. Each of these three phases has different activities, impacts, and results, all of which can be affected by the actions of end users.

As seen in the diagram below, the WACIRC (Washington Computer Incident Reporting Center) uses this 3 stage model for categorizing the phases of computer security incidents and the associated types of communications and actions from end users and customer agencies. This framework helps the end users and the WACIRC make the communications more efficient and effective during each phase of computer security incident handling.

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

WACIRC INBOUND COMMUNICATIONS FRAMEWORK[1]

SANS	WACIRC	COMMUNICATION	AGY TIMELINE
PREPAREDNESS	BEFORE	WACIRC/Security Contacts Chg Req	WHEN CONTACTS CHANGE
		Heads-up, FYI	WHEN INFO COMES AVAILABLE
		Potential Security Risk Report	WHEN DISCOVERED
IDENTIFY		Suspected Security Incident Report	WHEN DISCOVERED
CONTAINMENT	DURING	Security Health Check Report	WITHIN 60 MIN AFTER INCIDENT START
		Periodic Incident Status	ONGOING AND PERIODICAL
ERADICATION		Security Incident Eradication Status	WITHIN 30 MIN OF ERADICATION
		Security Incident Analysis Report	WITHIN 24 HOURS OF ERADICATION
RECOVERY	AFTER	Security Analysis Review	ANNUALLY - OCTOBER
LESSONS LEARNED		Security Gap Analysis	BIENNUALLY
		Security Best Practices Chg Req	WHEN NEED ARISES

Figure 2. WACIRC Inbound Communications Framework

BEFORE AN INCIDENT

Before an incident occurs, end users can unknowingly participate in the propagation of an incident in your environment or act as your remote agents in protecting your organization's security assets.

Recognizing Computer Security Incidents

Prior to a computer security incident occurring in your environment, your end users may have knowledge of the incident or the symptoms leading up to the incident. This type of information, when not reported, can retard the incident response team from determining an incident has occurred and may delay them from taking corrective action. Also, it allows exploits to propagate through your

[1] WACIRC Inbound Communications Framework

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

environment. The cause for many of the infections and successful exploits can come from inside your network. Frequently the impact is substantially magnified by uneducated end users. Some of them think they are opening a benign email or attachment. Some think they are downloading a cute little program to give them weather or stock updates, or display friendly screen saver. Some users aren't even aware that attachments, unsolicited commercial email (a.k.a. UCE), and emails from unknown sources are among the most common causes of viruses, trojans, worms and other malware. Even though the origin of these types of exploits and attacks may come from outside your network, the catalyst that allows them to propagate and run rampant through your network may very well be your own uneducated end users. If end users are educated about common security incidents and their symptoms, many of these types of incidents can be prevented from occurring in your environment. End users can also reduce the damage to your environment by recognizing the incidents and promptly report them to your CSIR Team.

Social Engineering

Lack of user education on the basics of computer security is one of the most common reasons for security breaches. A prime example of poor user education, the Mydoom worm used social engineering to propagate through networks.

> The worm masks the infected emails to look like system error messages, prompting people to click on them"[2].
>
> As of January 2004, according to F-Secure, a Helsinki Finland based security services organization, "Mydoom worm is now the worst email worm incident in virus history.[3]

One definition of social engineering goes something like this,

> Social Engineering..... the aim is to trick people into revealing passwords or other information that compromises a target system's security. [4]

Now, that is a fairly simple definition for social engineering. Below is a quote from an article published on the Security Focus web site that adds more detail on how social engineering can be applied in a computer security environment.

> Generally agreed upon as the weakest link in the security chain, the natural human willingness to accept someone at his or her word leaves many of us vulnerable to attack.[5]

[2] (F-Secure Incorporated)
[3] (F-Secure Incorporated)
[4] (Lexico Publishing Group, LLC)
[5] (Granger)

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

End users with security awareness training can help reduce or possibly eliminate social engineering from causing problems in your organization. The worst social engineering exploits ever recorded occurred because users did not recognize the symptoms. Social engineering is nothing more than taking advantage of uneducated end users.

Social engineering has worked its way into our email. Some of the most famous viruses in the history of the Internet were social engineered emails to get users to spread them. This is where end users, who aren't properly educated on security, can become your greatest risk by allowing viruses into your organization's environment. Lack of education on viruses allows end users to release them without knowing or even recognizing they have done so.

Viruses	First discovered
• Melissa, MS/Word macro virus in attachment to email.	(March 26, 1999)
• SirCam, arrives as attachment to an email message.	(July 17, 2001)
• Klez, worm propagates via email and network shares.	(April 17, 2002)
• W32.Swen.A, worm attaches to email & executes	(September 18, 2003)
• Mydoom, mass mail worm with executable attachment	(January 26, 2004)

All of these viruses, although originating outside most organizations networks, were spread with the help of uneducated users.

Not all forms of social engineering are electronic. The oldest and simplest form of social engineering is via telephone, where someone attempts to pass themselves off as an authority figure. Most people are inherently afraid of being reprimanded for not being cooperative. This can create a fertile environment for the would-be impersonator. An authority figure or security technician can persuade, cajole, or leverage an uneducated end user into giving up valuable information. Such information can eventually lead to a potential security breach later on by the authority figure impersonator.

People Making Mistakes

Contained in the list below, are the five most common mistakes made by end users. Most of these can be managed and/or monitored by a security or network support group. However, item # 2, "opening unsolicited email attachments……" is the most difficult to control. There are very few (if any), hardware or software solutions to prevent this. This type of incident is initiated solely by an end user.

The Five Worst Security Mistakes End Users Make

1. Failing to install anti-virus, keep its signatures up to date, and apply it to all files.
2. Opening unsolicited e-mail attachments without verifying their source and checking their content first, or executing games or screen savers or other programs from untrusted sources.

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3. Failing to install security patches-especially for Microsoft Office, Microsoft Internet Explorer, and Netscape.
4. Not making and testing backups.
5. Using a modem while connected through a local area network.[6]

Financial Impacts of Security Breaches

Uneducated end users can unknowingly shut down your entire business by disabling or hobbling the network with viruses, denial of services, and the like. The financial impact to your organization could be devastating.

> The mi2g Intelligence Unit [British computer-security firm] calculated the total economic damage in 2003 from all types of digital risk at between $183-billion (U.S.) and $224-billion worldwide. The equivalent economic damage figures for 2002 stood at between $106-billion and $130-billion.[7]
>
> Internet attacks in February [2004] caused an estimated $68 billion to $83 billion in damages worldwide, British computer-security firm mi2g reported. The damage estimates are about $50 billion higher than in January [2004], previously the most costly month on record.[8]

These same end users, when properly educated, can be the champions of your organization's security. Educating users on the importance their actions and the potential cost and damage of their mistakes could save your organization thousands of dollars in recovery costs, possibly even millions. Since the majority of these types of incidents are introduced by end users, the best method for preventing them is to provide proper security awareness education. End users who understand the potential damage that can be done by security incidents can also realize the potential risks.

Physical Security

Physical security is one of the least appreciated security disciplines. Frequently, the CSIR Team is not responsible for the physical security of an organization or even of specific buildings where security assets are located. Often, there is facility staff or security guards who have responsibility for physical security. End users seldom feel a responsibility for physical security. Vendors and visitors are frequently allowed access to work areas without identity validation, escorts, or instruction on rules for secured areas. Computer security depends very heavily on the physical security being strong, consistent, and comprehensive. Physical security is the first layer of security in the layered defense security model. If somebody can access the building or office where the security assets reside without proper authorization, they have just breached your first layer of security. Many security systems rely on the physical security as the first layer to ensure their security assets. Respecting the boundaries of the physical security systems

[6] (SANS Institute)
[7] (Kapica)
[8] (Lemke)

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

is recognition of the value physical security adds to the overall security plan. End users must be aware and must respect the physical security in order for the balance of the security system layers to work effectively for an organization.

Security and Acceptable Use Policies
What can you do to protect your organization's security assets? First of all, get the end users familiar with your security policies. If you are building new policies or updating the old ones, get your end users involved in the process.

Having a security policy that addresses the use of email and acceptable use for access to the Internet is important in defining what end users are allowed to do. However, having a security policy and/or procedures without the education of the end users is like having a door on your house, but nobody closes it. The end users don't know the door is supposed to be closed. They don't know the value of the contents inside the door, so they don't know how important it is to keep the door closed. Additionally, the valuables behind the door are not owned by the end users, so they have less interest in protecting them.

Getting the end users involved in the incident handling process from the beginning is imperative to get them to take ownership of the organizations security. Most end users have not seen the risk management plan. They don't know of the valuables behind the door. They don't realize how they can be negatively affected by a breach of security. End users don't know how they can participate in the overall security. Better yet, they don't know what individual loss they may encounter, if the entire organization isn't adequately secured.

DURING AN INCIDENT
During the incident, when the incident is attacking or spreading through your network or environment, end users can be either adding to the CSIR Team's misery by their actions, or they can be assisting in the battle with the incident.

Unnecessary Delays
When end users are not aware of the impact of computer security incidents, they can complicate matters through their own curiosity, by attempting to gather information on the incident. This activity can add unnecessary traffic, which in turn, may further congest the very network you must use to fight the incident, clean the infected devices, isolate the cause, or download patches to correct the problem. Also, this activity can dilute or negate the actions of the CSIR Team by increasing the number of suspect packets or transmissions which must be monitored for the potential cause or propagation of the incident. This can increase the time spent by the CSIR Team in identifying the actual source and delay the containment or eradication of the incident.

Timely Reporting and Response
When a CSIR Team is responding to an incident, time is extremely valuable. Every second counts. For every second an incident is allowed to exist in your

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

environment, it is one more second the incident can be doing damage. Every second that is lost by CSIR Team in combating the incident can translate to more damage, more financial or reputation loss to the organization, and more people time needed to correct the problem.

This is where educated end users can prevent or reduce the spread of incidents in your environment, by recognizing incident symptoms and reporting them, promptly. This enables the CSIR Team to respond more quickly and begin the containment process for the incident. The sooner the CSIR Team can respond to the incident, the less damage the incident may do to your organization's valuable data. Instead of adding to the CSIR Team's problems, end users can be valuable "sensors" by reporting back to the CSIR Team on any abnormalities they observe, as quickly as possible. Reporting changes can help the CSIR Team identify where their efforts are having an effect and where they should focus to contain and eradicate the incident in a timely fashion.

Providing comprehensive reporting mechanisms and educating end users on how to use them, gets the important information about the incident to the CSIR Team much faster, enabling them to respond faster.

Opening the Door for Slammer

End users may not be able to stop the infiltration by a security incident, but they can react in a timely manner. Once an incident is inside your environment, it can spread so quickly that humans can't possibly block it, but they can mitigate the impacts if they react timely and report the incident immediately. A good example of this is the Slammer worm.

> The Slammer worm spread so quickly that human response was ineffective. In January 2003, it packed a benign payload, but its disruptive capacity was surprising. Slammer (sometimes called Sapphire) was the fastest computer worm in history. As it began spreading throughout the Internet, the worm infected more than 90 percent of vulnerable hosts within 10 minutes.

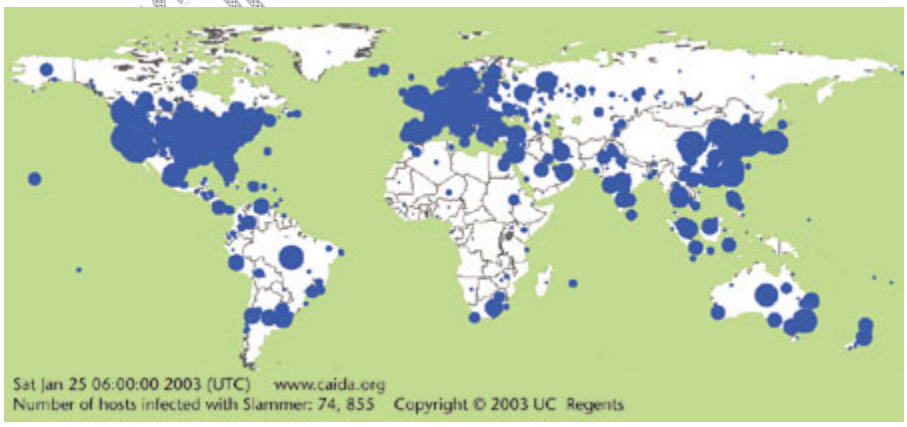


Figure 3. Geographical spread of Slammer in 30 minutes after its release.

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

> Slammer's 376 bytes comprise a simple, fast scanner with its requisite headers. The payload becomes a single 404-byte user diagram protocol (UDP) packet. Contrast Slammer's 404 bytes with Code Red's 4 Kbytes or Nimda's 60 Kbytes.[9]

If one of your users were to unknowingly unleash a virus with the distribution potential of Slammer and a destructive payload, your organization could be catastrophically damaged within minutes. Educated users can help prevent this type of incident from occurring by recognizing the common symptoms and patterns of incidents, and reporting them timely. This can only be done if end users are educated on security incidents and proper response procedures and reporting mechanisms.

Overloading Valuable Security Resources

When end users use the network to satisfy their curiosity of what is happening, or utilize organization's resources unnecessarily during a security incident, the resources are not available for use by the CSIR Team to solve the problem. By using critical incident response resources during an incident, like computer equipment, internet connections and network bandwidth, end users can limit one of the most important components of security; resource availability.

Common Incident Types and Symptoms

If end users understood the impacts computer security incidents can have on organizations networks and security resources, they would be better able to assist the CSIR Team during an incident. Not understanding the importance of security, different types of security incidents and the most common symptoms, can delay end users from reporting incidents timely. This, in turn, delays the response of the CSIR Team and allows the incident to spread or cause more damage to an organization. Lack of education on incident symptoms and potential damages caused by them, may invite end users to take actions that could delay the CSIR Team in responding to the incident.

End users having a basic understanding of security exploits can be the best defense an organization can have. Preventing the exploit from getting in, and reporting symptoms immediately upon their discovery can be the most valuable actions end users could take during an incident. Most end users don't know about types of basic security incidents and their symptoms. This information would empower every employee to be a secure conscientious user.

Patch Management

In some organizations, end users are responsible for patching their own systems. A classic example of this is when an organization allows employees to connect to their network from the employee's home computer. When this happens the home user can become the responsible agent for applying operating system and application program updates, service packs, and antivirus system and signature

[9] (Moore et al.)

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

file updates. The health of the organization's network can become dependant on the end users ability to recognize the security incident and take appropriate corrective action to respond to it. End users, who don't patch or update their systems in a timely fashion, can put the entire organization's network at risk. End users must understand the impacts and consequences of not keeping their systems patch and update properly.

AFTER AN INCIDENT

After the incident has been contained and eradicated, end users can become the most valuable assets you have, or they can be destined to repeat the mistakes already made. In all phases of incident response the action or inaction of your end users can affect the fate of your organizations security.

Recording and Documenting

At this point you enter the recovery phase. This is the phase where we collect all the information that was documented on the security incident and analyze it to formulate conclusions about the nature of the security incident. While most system administrators are trying to rebuild, reboot, or restore services and data, you can be assembling data about the incident from your end users. This data can help explain the method in which your security was breached, if your end users have taken the time and effort to document it. If end users don't collect data, or collect incomplete data, you may never be able to isolate the cause of the incident or prevent it from recurring. Educated end users can assist in identifying the incident cause or origination by collecting data on events occurring during the incident. End users, who collect accurate and correct data, can be the single most important element to identifying the cause of an incident, and thus help in the building of a robust layered security defense.

If end users understand the importance of documenting symptoms and events during a security incident, they can collect valuable information relevant to the incident. When you begin the recovery phase, you can call upon their logs or knowledge to build a much bigger and clearer picture of the incident. This way you may be able to determine the incident's entry point and the way it propagated through your environment. Sometimes the review of end user's logs connects what seem to be unrelated facts about the incident.

Impact Assessment

When it comes to determining the damage or impact of the security incident, the end users have the best view of what happened at the business end of the organization. They can tell you which systems were affected and which were not during the security incident. The end users can tell you where they were prevented from delivering services to customers, where they could not do their jobs due to the security incident. The end users can give the CSIR Team a much better idea of the actual impact to the organization's business, and the affects it had on the organization's customers.

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Not only will end users have a first hand view of the events that occurred during an incident, but they will gain broader understanding of the actions taken by the CSIR Team to remedy the security incident. Involvement in the incident impact assessment gives end users a valuable perspective of the processes and procedures currently in place to deal with computer security incidents, and where they may be able to help.

Post Incident Review
End users who participated in the security incident response, along with those who recognized the symptoms and effects should be involved in the preparation, the review, or both aspects of the Post Incident Report.

The benefit of doing this is in the gathering of the pertinent information about the incident and analyzing how the security was breached so it can be prevented from occurring in future. End users can contribute valuable information to the cause and symptoms of a security incident. If end users are educated, they can log anomalies and abnormal behavior of the computer systems they use, which may give the CSIR Team an insight to the origin of the incident. Once end users see how important data collection becomes during a security incident, they can be the "early warning system" for the CSIR Team on future incidents. This can improve the communication process for incident response on which we are so dependant, by having the end users know what to report and when to report it. The key to a successful Post Implementation Review is found in the incident debriefing reports completed by the end users. If end users have comprehensive incident debriefing tools and reports, they can provide prompt and accurate descriptions of events related to the occurrence of the security incident.

Lessons Learned
End users must learn from their experiences with security incidents, so they can avoid falling victim to these types of situations in the future. The simplest method of learning for most people is from their own mistakes. If the end users are not involved in this phase of incident handling, they might negatively impact future incident handling processes by their lack of security awareness. There is an old saying that gives us direction for this phase of incident handling.

> He, who ignores the past, is destined to repeat it – Ancient proverb.

Heeding the advice of this proverb may prove to be the most valuable lesson we could ever learn in the computer security business.

Applying Lessons Learned to Policy and Procedures
As with all security processes, review by the widest security audience possible, maximizes the strength of a process. The value gained by involving the end users in Post Incident Review and the resulting changes to an organization's security program, policies, processes, and procedures is similar to the value gained by involving the end users in the development of any system or service

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

utilized by them. This success of this process of involving end users in development of the end product has been proven and documented in the computer applications development cycle. As quoted by James Martin, an industry recognized expert in the IT field,

> The more thinking, iteration, and interaction with the users, that goes on before a [system] is implemented, the better the final product will be.[10]

Action plans, process improvements, and procedural and policy changes will be accepted and utilized by the end users with much more commitment, if they are involved in the development and implementation. Obtaining end users buy-in for changes in their environment becomes a much easier task, when the end users helped develop the changes. Therefore, end user involvement in Post Incident Reviews and resulting policy, procedure and process improvements is an important milestone on the path to true improvement for the security incident response process.

Growth of Security Responsibility

In the past the security group, the CSIR Team, and organization's management were responsible for maintaining the security of the organization's assets. Today, that responsibility has grown to include all employees and all users. Despite what end users think about their responsibility, everyone within an organization has some responsibility for its security. Whether it translates to questioning an unfamiliar face in the building, keeping your personal security information (i.e. passwords, logins, etc.) confidential, or making sure you don't open that unknown email, everyone within an organization has a responsibility to help maintain the security. Getting end users involved in the changes to an organization's security, and action plans resulting from a Post Incident Review, will help them step up and support the security rules.

WHAT CAN BE DONE TO IMPROVE END USER SECURITY AWARENESS?

There is a point where you must determine what you can change directly and what you must change through others. All the hardware and software in the world can prevent only some of your security problems. If your end users do not understand basic security and their responsibility in securing the organization, they will always be a security risk for your organization.

Uneducated end users are the weakest point in the security armor, and the point where you have the least control. Therefore, the best solution is to educate them to be part of the security defense layer. "Deputize" your end users to take certain actions to prevent, reduce, mitigate, report, and respond to security incidents. Educate them to take the correct actions at the correct time. Use them as remote agents for the CSIR Team and the security group. Show your end users the penalty your organization pays for security breaches. Show them the drawbacks of not taking corrective action in a timely manner.

[10] (Martin 255)

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

HOW DO YOU EDUCATE END USERS ON SECURITY?
End users can do several things to assist the CSIR Team in fighting a computer security incident. From the time prior to an incident occurring through to the final eradication, recovery and review of the incident, end users can participate in the process of incident response. Listed below are some solutions organizations can employ to make end users more effective, and things end users can do to make the organization more effective at incident handling. All of these solutions are directly related to security awareness education of end users.

What Can Be Done BEFORE a Computer Security Incident
By Organizations:

- Teach your end users when to report an incident.
- Post common security incident symptoms and patterns.
- Instruct end users on common incident symptoms and patterns.
- Show end users what data to report
- Show end users what NOT to report
- Instruct end users when to report an incident.
- Post the "Do's and Don'ts" of organization computer security.
- Perform a risk analysis of your computer security infrastructure.
- Perform a security asset inventory.
- Implement automated patch distribution system, if applicable.
- Post financial impacts of previous incidents for end users.
- Instruct end users on basic incident response process and communications.
- Identify secured areas and post rules for accessing them.
- Implement a security policy for acceptable use of email.
- Implement a security policy for the acceptable use of Internet access.
- Inform and periodically remind users of security policies.
- Get the end user's involved in the incident handling process early.
- Show them the risk management plan.
- Make them aware of the valuables behind the door.
- Show end users how they can be affected by the breach of security.
- Show end users how they can participate in the overall security.
- Show end users the individual loss they may experience, if the entire organization isn't adequately secured.

By End Users

- Learn your role in a security incident.
- Learn about common security incidents.
- Learn and recognize specifics about "social engineering".
- Participate in computer security exercises, tabletops, and communications tests.
- Don't use weak or easily guessed passwords.
- Maintain logins/passwords confidential (no posting, sharing, or divulging)

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Don't use same or similar passwords for internal and external applications (local network login, web page login, etc.).
- Respect physical security rules and policies.
- Question unauthorized personnel in your facility.

What Can Be Done DURING a Computer Security Incident.
By Organizations:

- Notify your end users immediately.
- Keep your end users apprised of the current state of the incident.
- Accept feedback and input from your end users.
- Investigate all end users claims, regardless of appearances or severity.
- Provide vehicles for outbound and inbound communications.
- Require strict physical security and only authorized access to secure areas.
- Provide mechanisms for users to report security incidents.

By End Users:

- Don't use valuable network bandwidth unless absolutely necessary.
- Don't try to investigate the incident unless you are part of the CSIR Team.
- Don't attempt new or complex processes or applications.
- Report any and all changes, anomalies, abnormal or suspicious behavior of computer systems, networks, or applications programs to the CSIR Team in a timely manner.
- Keep a log of any an all abnormal activities or symptoms with time/date stamps.
- Check your workstation log for abnormalities, if applicable.
- If end users are responsible for patching their own systems, have the patches downloaded, tested, and installed as soon as they are available.
- Respect and follow physical security rules.
- Work with the CSIR Team, not against them.

What Can Be Done AFTER a Computer Security Incident.
By Organizations:

- Involve end users in a "lessons learned" process.
- Provide communication vehicle for incident debriefing and impact.
- Educate users of the consequences of previous security breaches.
- Post reminders of the risk, symptoms, and penalties of a security breach.
- Educate end users on the success and commonality of social engineering.
- Advise end users that they are susceptible to social engineering.
- Exercise social engineering tactics to enhance end user security education.
- Recognize HIPAA and other information security standards and requirements.
- Provide resistance training for public/customer facing employees (help desks, customer service, receptionists, etc.).

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

By End Users:

- Provide input to “lessons learned” process.
- Review and provide feedback to incident debriefing summary.
- Participate in process improvement meetings.
- Participate in the application of lessons learned and improvements to the security incident handling process, procedures, or policies.
- Educate end users on lessons learned after Post Incident Reviews.

CONCLUSION:

End users who are NOT educated on security can be the worst liability to any security defense.

On the other hand, educated end users can be the greatest asset we have in any security defense. Teach them! Use them! Reward them!

Educate your end users to be cognizant, reactive, and effective before, during and after a computer security incident. Provide direction for them to take the appropriate action during a security incident. Remind them there are three paths to take in the process of becoming a valued end user for incident handling:

1.) LEAD – take a proactive stance on security, personally and within your immediate group. Take responsibility for your own computer security.

2.) FOLLOW – take direction from the CSIR Team or the security team on what you can do to help them respond to incidents effectively.

3.) GET OUT OF THE WAY – don’t do things that delay or confuse the CSIR Team’s efforts to handle the incident, or cause the incident to propagate.

©SANS Institute 2004, Author retains all rights.

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

REFERENCES:

Northcutt, Stephen. SANS Step-by-Step Series: Computer Security Incident Handling. Version 2.3.1. SANS Press, 2003.

F-Secure Incorporated. "Mydoom worm is now the worst email worm incident in virus history." 28 Jan 2004. URL:
URL: http://www.f-secure.com/news/items/news_2004012800.shtml (20 Mar 2004).

Lexico Publishing Group, LLC. "Dictionary.com." 14 Sep 2000. URL:
http://dictionary.reference.com/search?q=social%20engineering (20 Mar 2004).

Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics." 18 12 2001. URL: http://www.securityfocus.com/infocus/1527 (20 Mar 2004).

SANS Institute. "Mistakes People Make that Lead to Security Breaches." 23 Oct 2001. URL: http://www.f-secure.com/news/items/news_2004012800.shtml (20 Mar 2004).

Kapica, Jack. "Cyber attacks on rise after Hussein capture." The Globe and Mail 22 12 2003. URL:
http://www.globetechnology.com/servlet/story/RTGAM.20031222.gtattack1222/BNStory/Technology/ (21 Mar 2004)

Lemke, Tim. "Computer viruses, worms set costly Internet record." Washington Times 01 Mar 2004. URL: http://www.washtimes.com/business/20040229-105349-9778r.htm (21 Mar 2004)

Moore, David, Vern Paxson, Stefan Savage, and Colleen Shannon. "Slammer Worm Dissection: Inside the Slammer Worm." Security & Privacy.
URL: http://www.computer.org/security/v1n4/j4wea.htm?SMIDENTITY=NO
(21 Mar 2004)

Martin, James. Information Engineering, Book II: Planning and Analysis. 1st ed. Englewood Cliffs: Prentice-Hall, Inc, 1990.

Smith, Kevin. "About Viruses: All you ever wanted to know about computer viruses." Case Western Reserve University. 09 Apr 2004.
URL: http://help.case.edu/safe/maintain/virus/about/view

Rusch, Jonathon J. "The "Social Engineering" of Internet Fraud." INET '99. United States Department of Justice. 12 Apr 2004.
URL: http://www.isoc.org/inet99/proceedings/3g/3g_2.htm

"Incident Handling Checklists." Federal Computer Incident Response Center. U.S. Department of Homeland Security. 12 Apr 2004.
URL: http://www.fedcirc.gov/incidentResponse/IHchecklists.html

SANS Institute 2004 As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.