

Information Assurance Awareness

A Quick User's Guide To Incident Response

June 2011

It All Starts With You:

It may seem hard to believe, but users are nearly always most effective in discovering when bad things happen. Even with modern antivirus programs, firewalls, and automated intrusion detection systems, most computer incidents are detected by the end user and not by any centralized technical measures. All users need to be vigilant for unusual system behavior, which may indicate a security incident in progress.

"Events" and "Incidents":


An "event" is any observable occurrence in a system and/or network. Examples of events include erratic behavior, unusual system crashes, strange pop-up windows, inability to connect to resources, or data that has been inexplicably changed or missing. Events can be caused by many things such as power-related disruptions, floods, fires, and excessive heat can cause crashes and data loss. Events can also be caused by human error (such as unintentionally deleting a folder or file). As costly and disruptive as these types of events are, they are not referred to as "incidents"


The term "incidents" refers to an adverse event that is INFOSEC related. Events sometimes provide indication that an incident is occurring. Computer security-related events, however, are attracting an increasing amount of attention within the Army and DOD.


Types of Incidents:


The term "incidents" refers to an adverse event in an information system and/or network or the threat of the occurrence of such an event.


Some of the different types of incidents can be described using the following general categories of adverse events:


 **Malicious code.** Malicious code include attacks by programs such as viruses, Trojan horse programs, worms, and scripts used by to gain privileges, capture passwords, and/or modify system files and/or data.

 **Unauthorized access.** Unauthorized access occurs when someone (or something) gains logical or physical access without permission to a network, system, application, data, or other IT resource. This ranges from logging onto the network using someone else's account to obtaining elevated privileges in order to view files and directories. It also includes access to network data through "sniffer" programs or devices to capture network traffic.

 **Disruption of service.** Perpetrators and malicious code can disrupt these services in many ways, including erasing a critical program, "mail spamming" (flooding a user account with electronic mail), and altering system functionality by installing a Trojan horse program.

 **Misuse.** Misuse occurs when someone uses a computing system for other than official purposes.

 **Espionage.** Espionage is stealing information to subvert the interests of a corporation or government.

 **Hoaxes.** Hoaxes occur when false information about incidents or vulnerabilities is spread.

Note that these categories of incidents are not necessarily mutually exclusive. A hacker from a remote country could run malicious code to obtain unauthorized access to a system for the purpose of espionage.

User Responsibilities :

All authorized users of the Fort Lee network are responsible for:

- Taking the appropriate actions when a security anomaly is noted or suspected.
- Reporting actual or suspected security violations or incidents to their local IASO and/or supervisor.
- Participating in annual IA Awareness training and Authorized Use Policy (AUP) renewal.
- Knowing what actions to take if an incident is suspected.

Actions to Take if An Incident is Suspected:

1 STOP !

Stop working. Do not attempt to save, copy or access files and/or folders. Prevent any additional activities on the system. This includes execution of back-up programs, drive/disk defragmentation, deletion of temporary files, emptying items from the wastebasket of the user profile, etc. Do not attempt to run any third-party forensic or cleaning/repair tools without the direct authorization of the ACERT or RCERT-CONUS. These types of actions may alter files and destroy potential evidence or intrusion indicators.

2 DROP !

Isolate the system immediately. Remove/unplug the network cable from the system. DO NOT turn the power off or unplug the power cable from the system. Turning the power off may potentially destroy any forensic evidence that may be present in the volatile memory, temporary files, or in the “run once” registry settings. Restrict access to the system by other users.





3 CALL !

Notify your local organization IMO, IASO, or supervisor immediately. Tell them what happened. Provide as much information as you can about what you were doing, what programs you were using, what file or website you were accessing. All of this information is needed in order to determine exactly what has happened and what actions need to be taken next.

Want More Information?

The first step is your local organization’s Incident Response Plan. It contains instructions, actions, and procedures specific to your organization.

Other sources for additional information include:

-  AR 25-2, Information Assurance (<http://www.apd.army.mil>)
-  Army Computer Emergency Response Team (ACERT) website (<https://www.acert.1stiocmd.army.mil/index.jsp>)
-  Fort Lee Incident Response Plan (`\\vs\public\Documentation\ICAN_Documentation`)
-  Annual IA Awareness training (<https://ia.signal.army.mil>)