



# Incident Response & Evidence Management

CIPS Brandon Chapter  
November 28 2002



Dr. Marc Rogers PhD, CISSP

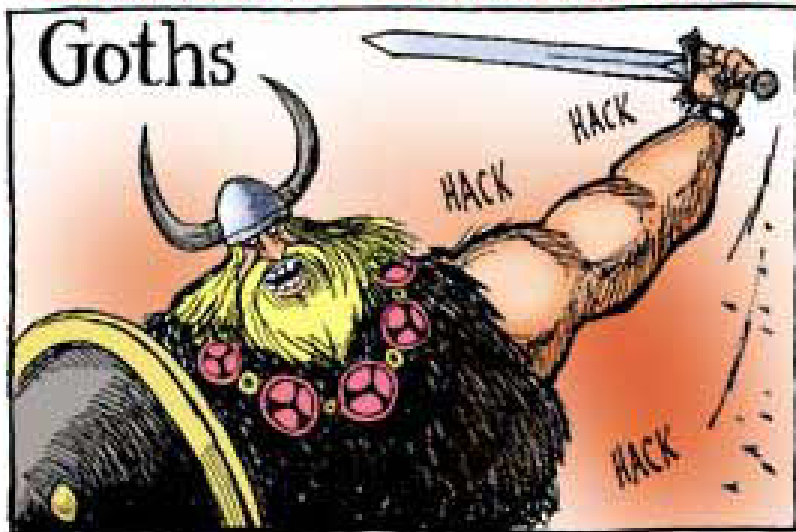


# Agenda

- Current State of the IT World
- What is Incident Response
- What is Evidence Management & Handling
- Tie into DRP/BCP
- Summary



# BRINGING CIVILIZATION TO ITS KNEES...



KEVIN STERS ©2000 THE CHARLOTTE OBSERVER



# Hong Kong Reuters Office Hacked:

banks lose price data  
36 hours

PA Teenager Charged With 5 Counts of Hacking:  
Southwestern Bell, BellCore, Sprint, and SRI hit  
Costs to Southwestern Bell alone exceed \$500,000

**c|net** **CNET NEWS.COM** TECH NEWS FIRST

CNET : [News](#) : [E-commerce](#) : [Story](#)

[Market Update](#) | [My Portfolio](#) | [Broker Reports](#) | [Tech Sectors](#)

## De Beers security hole reveals customer information

By [Stefanie Olsen](#)  
Staff Writer, CNET News.com  
April 4, 2000, 4:45 p.m. PT

**On the Web, diamonds can be a spammer's best friend.**

About 35,000 customer email and home addresses were exposed on Adiamondisforever.com, an informational site about diamonds. De Beers, CNET News.com has learned.

Million Hack:  
inside help.  
net recovered.

Computer At  
40 hour shutdo

Web Sites  
g season

**Technology terror**  
10 products that will sc

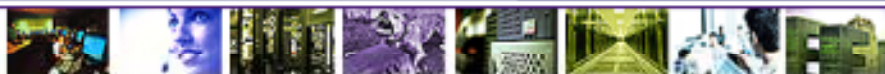
**Facts**

**Back Office**  
system requirements:  
88, Windows 95 or 98,

**10. Back**

**Trick:** Allows someone to control your PC remotely--without authorization.  
**Treat:** Your archenemy deletes your files just for the heck of it.

Ships Infected  
PCs:  
Virus Taints Big Japanese  
Debut



# The Net

◀ back to

## AOL outage brief but dangerous

By [Janet Kornblum](#)  
Staff Writer, CNET NEWS.COM  
February 24, 1998, 1:00 p.m. PT

**news analysis** The last time [America Online \(AOL\)](#) suffered a total blackout, members were knocked offline for 19 hours. Last night's [outage](#) by comparison, lasted a relatively painless 2-1/2 hours.

In the long run, however, the latest disruption underscores a more lasting problem for the online giant. An outage of any significant duration at a time when AOL so dominates the market may leave



NEWS.COM  
front page

Join now FREE!

MENU

# The Net

◀ back to

## Student finds AOL bug

By [Janet Kornblum](#)  
Staff Writer, CNET NEWS.COM  
February 24, 1998, 4:35 a.m. PT



Feb. 25, 1998 >> 1:34 pm EST

Stephen Cobb's

## custom:news

# Pentagon says computers invaded by hackers

February 25, 1998  
Web posted at: 10:26 a.m. EST (1526 GMT)

- Custom News ▾
- Home
- World
- U.S.
- Weather
- Sports

**fn** small business tool kit.  
click here

Washingtonpost.com: Computer Glitch Halts NYSE Trading for One Hour - Netscape

File Edit View Go Communicator Help

HOME INDEX SEARCH ARCHIVES **9.9% Fixed (not an introductory rate!)**  
No Annual Fee  
NEWS STYLE SPORTS CLASSIFIEDS

**\$10 OFF**  
  
Partners:  
**Newsweek.com**  
Britannica-Newsweek Internet Guide

## Computer Glitch Halts NYSE Trading for One Hour

By *Ianthe Jeanne Dugan and Mark Leibovich*  
Washington Post Staff Writers  
Tuesday, October 27, 1998; Page C01

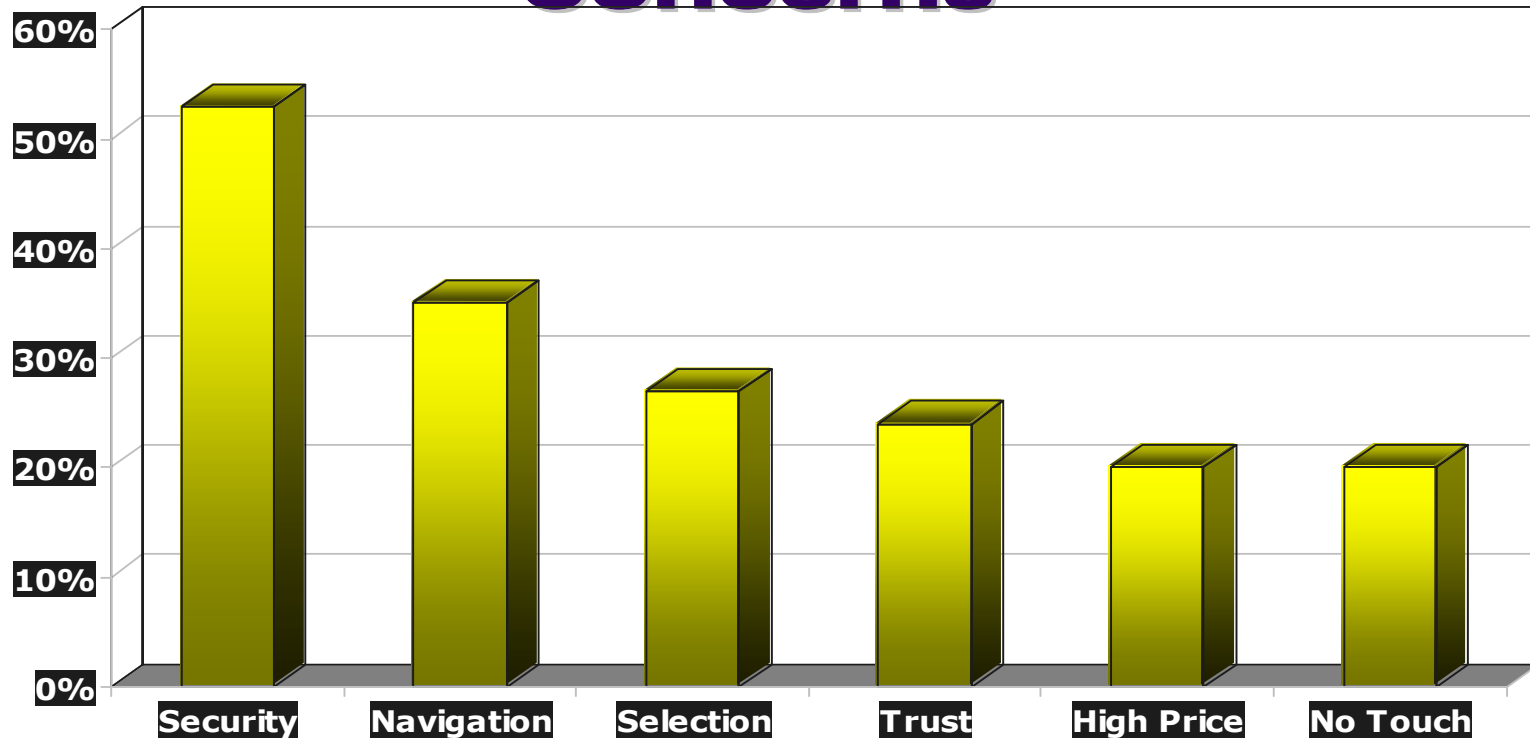
Stocks froze in their tracks for an hour yesterday on the New York Stock Exchange after an unusual computer glitch forced exchange officials to shut



two civilian official.



# Consumer e-Commerce Concerns



*Privacy/Security issues could potentially put an \$18 billion dent in the projected \$40 billion 2002 e-Commerce revenue (Jupiter Communications, 2000).*

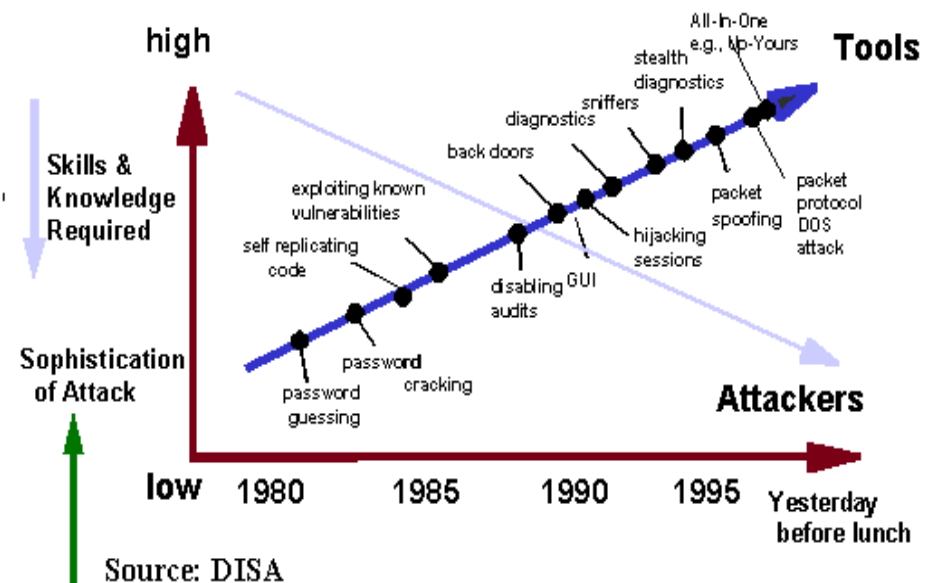


# Attackers

- Attacks are becoming more sophisticated

Progressed from simple user command, script and password cracking (sniffers, crackers) in 1993-94, to intricate techniques that fooled the basic operations of IP (spoofing etc.)

- But Attackers less skilled





# CSI/FBI 2002 Survey

- 90% of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.
- 80% acknowledged financial losses due to computer breaches.
- 223 respondents reported **\$455,848,000** in financial losses.
- 74% cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).
- 34% percent reported the intrusions to law enforcement. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)





# Incident Response Goals

- Provide an effective and efficient means of dealing with the situation in a manner that reduces the potential impact to the organization.
- Provide management with sufficient information in order to decide on an appropriate course of action.
- Maintain or restore business continuity.
- Defend against future attacks.
- Deter attacks through investigation and prosecution.



# Relationship to InfoSec

- The IAC triad can be expanded to include:
  - Non-repudiation
  - Accountability
- Incident Response is directly linked to InfoSec goals
- It can help restore the IAC

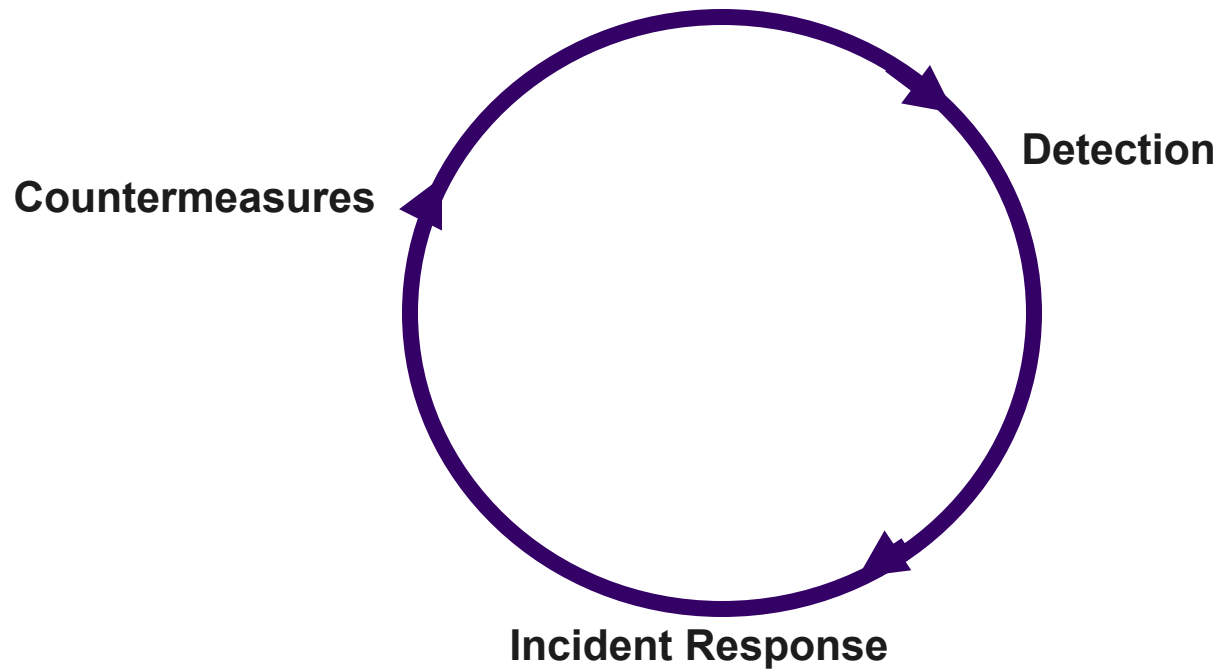


# Information Security Lifecycle

- Countermeasures
  - Defenses that counter threats
  - No defenses are fool proof
- Detection
  - Indicates that security has been breached
- Incident Response
  - After the incident has been noticed responding to it is critical



# Information Security Lifecycle



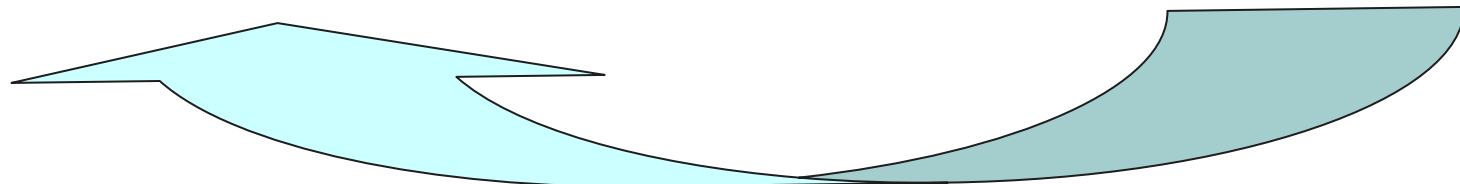


# Seven-Stage Methodology

- Methodology has been around since about 1989
- DOE under Dr. Schultz matured the model
- Definitely not the only method
- Has become part of the Common Body of Knowledge
- Very pragmatic & logical approach
- Although presented as a linear model some stages may happen in parallel or like the “waterfall” method feedback into the previous stages



# Response Methodology (PDCAERF)



Feed Back



# Response Methodology

- Why use a methodology?
- Structure/Organization
  - Dealing with incidents can be chaotic
  - Simultaneous incidents occur
  - Having a predefined methodology lends structure to the chaos
- Efficiency
  - Time is often of the essence when dealing with incidents
  - Incidents can be costly both financially and organizationally



# Response Methodology

- Process oriented approach
  - Breaks incidents into small manageable chunks
  - Logical order of dealing with issues
  - Includes methods for improving the overall process
- Dealing with the unexpected
  - Provides a mental framework for dealing with incidents in general
  - Promotes flexible thinking to deal with novel situations





# Response Methodology

- Legal Considerations
  - Can demonstrate due care or due diligence
  - May limit liability
  - May reduce insurance premiums



# Evidence Management

- During an incident, evidence may be collected during any of the 7 phases.
- In early stages we may not know what the final outcome might be (e.g., Job Termination, Civil or Criminal Litigation).
- Network/Computer Forensics may become an issue
- Must collect data in a “Forensically Friendly” manner
- Must maintain the chain of custody
- Important to understand the evidence lifecycle



# Forensics

- [Computer Forensics](#): The study of computer technology as it relates to the law.
- [Forensic Analysis](#): Examination of material and/or data to determine its essential features and their relationship in an effort to discover evidence in a manner that is admissible in a court of law; post-mortem examination.



# Forensics



- Electronic Evidence:

Evidence relating to the issue that consists of computer files, or data, in their electronic state.

- Electronic Media Discovery:

The discoverability of electronic data or files.



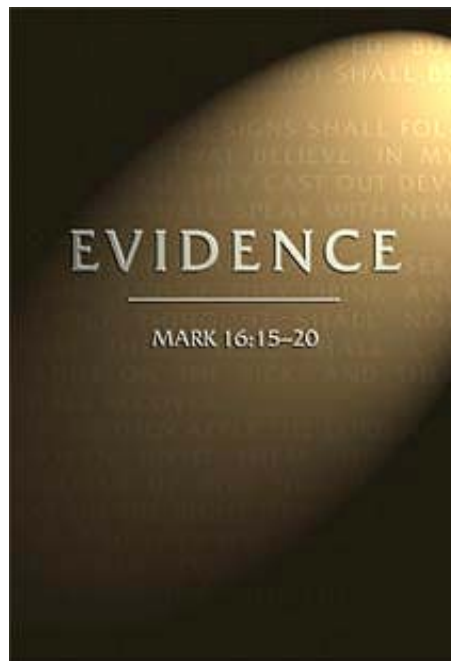
# Forensics

- Chain of Custody: A means of accountability, that shows who obtained the evidence, where and when the evidence was obtained, who secured the evidence, who had control or possession of the evidence.
- Rules of Evidence: Evidence must be competent, relevant, and material to the issue.





# Evidence Life Cycle



- Collection & identification
- Storage, preservation, and transportation
- Presentation in court
- Return to victim or court



# IR & DRP/BCP

- Both IR & DRP/BCP use planning and preparation to mitigate the damage of an negative event after it occurs.
- Both require fore thought, formal written policies, procedures, and budgets.
- Both rely on periodic testing and maintenance of the plan.
- IR can be a subset of DRP/BCP process.



# Summary

- The rate of network/computer intrusions is increasing
- Most companies/organizations have safeguards such as firewalls, Anti-virus, IDS
- We need to know what to do when the alarms go off
- Like DRP/BCP we must have a IR plan in place before hand
- Proper evidence management & handling procedures are important during the response escalation process
- IR is the next evolution of the IT Security Industry





# Contact Information

Dr. Marc Rogers PhD., CISSP

Ph: 989-8750

E-mail: [mkr@manageworx.com](mailto:mkr@manageworx.com)

Web: [www.manageworx.com](http://www.manageworx.com)





# Book References

- Kruse, W. & Heiser, J. (2002). Computer forensics: Incident response essentials. Boston: Addison Wesley.
- Mandia, K. & Proise, K. (2002). Incident response: Investigating computer crime. New York: Osborne/McGraw Hill.
- Northcutt, S., & Novak, J. (2002). Network intrusion detection: An analyst's handbook 2nd edition. Boston: New Riders
- SANS. (2001). Computer security incident handling: Step-by-step. The SANS Institute.
- Schultz, E., & Shumway, R. (2002). Incident response: A strategic guide to handling system and network security breaches. Boston: New Riders.



# Web References

- CERT/CC [www.cert.org](http://www.cert.org)
- CERT/AU [www.uscert.org.au](http://www.uscert.org.au)
- OCIEPEP [www.ociepep-bpiepc.gc.ca](http://www.ociepep-bpiepc.gc.ca)
- CERIAS [www.cerias.purdue.edu](http://www.cerias.purdue.edu)
- FIRST [www.first.org](http://www.first.org)
- SANS [www.sans.org](http://www.sans.org)
- INCIDENTS [www.incidents.org](http://www.incidents.org)
- CCIPS [www.cybercrime.gov](http://www.cybercrime.gov)
- IIC [www.iic.umanitoba.ca](http://www.iic.umanitoba.ca)
- RCMP [www.rcmp-grc.gc.ca](http://www.rcmp-grc.gc.ca)
- FORENSICS [www.incident-response.org](http://www.incident-response.org)