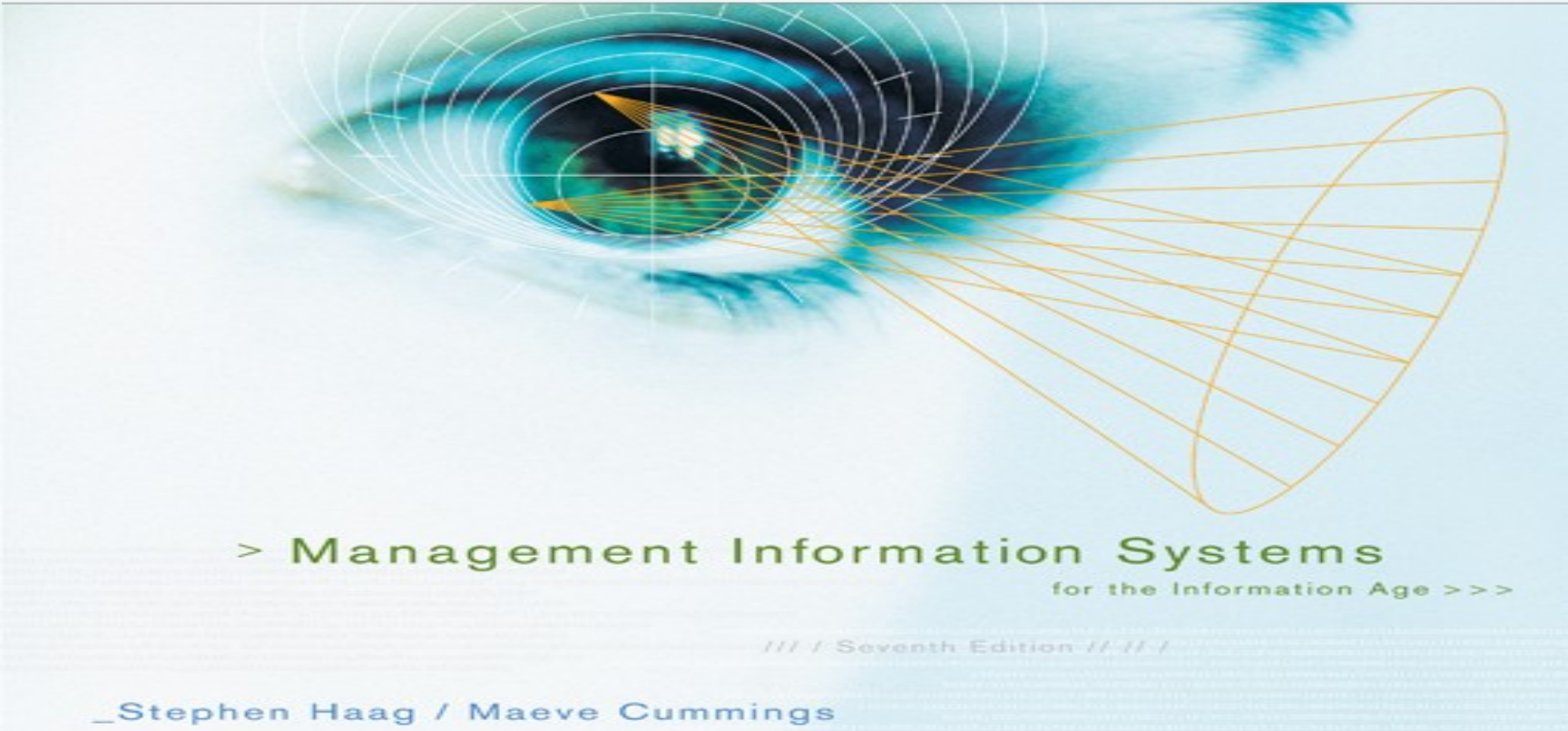
Extended Learning Module H
COMPUTER CRIME AND DIGITAL FORENSICS



STUDENT LEARNING OUTCOMES

1. Define computer crime and list three types of computer crime that can be perpetrated from inside and three from outside the organization
2. Identify the seven types of hackers and explain what motivates each group
3. Define digital forensics and describe the two phases of a forensic investigation

STUDENT LEARNING OUTCOMES

1. Describe what is meant by anti-forensics, and give an example of each of the three types
2. Describe two ways in which corporations use digital forensics

INTRODUCTION

- Computers are involved in crime in two ways
  - As the targets of misdeeds
  - As weapons or tools of misdeeds
- Computer crimes can be committed
  - Inside the organization
- Outside the organization

MODULE ORGANIZATION

1. Computer Crime
   - Learning Outcomes #1 & #2
2. Digital Forensics
   - Learning Outcome #3
3. Recovery and Interpretation
   - Learning Outcome #4
4. Who Needs Digital Forensic Investigators?
   - Learning Outcome #5

COMPUTER CRIME

- ***Computer crime*** – a crime in which a computer, or computers, play a significant part

Examples of Computer Crimes

Crimes in Which Computers Usually Play a Part

- Illegal gambling
- Forgery
- Money laundering
- Child pornography
- Hate message propagation
- Electronic stalking
- Racketeering
- Fencing stolen goods
- Loan sharking
- Drug trafficking
- Union infiltration

Outside the Organization

- In 2006 the greatest financial loss stemmed from
  - Virus and worm attacks
  - Unauthorized access
  - Theft of hardware
  - Theft of information
  - Malware

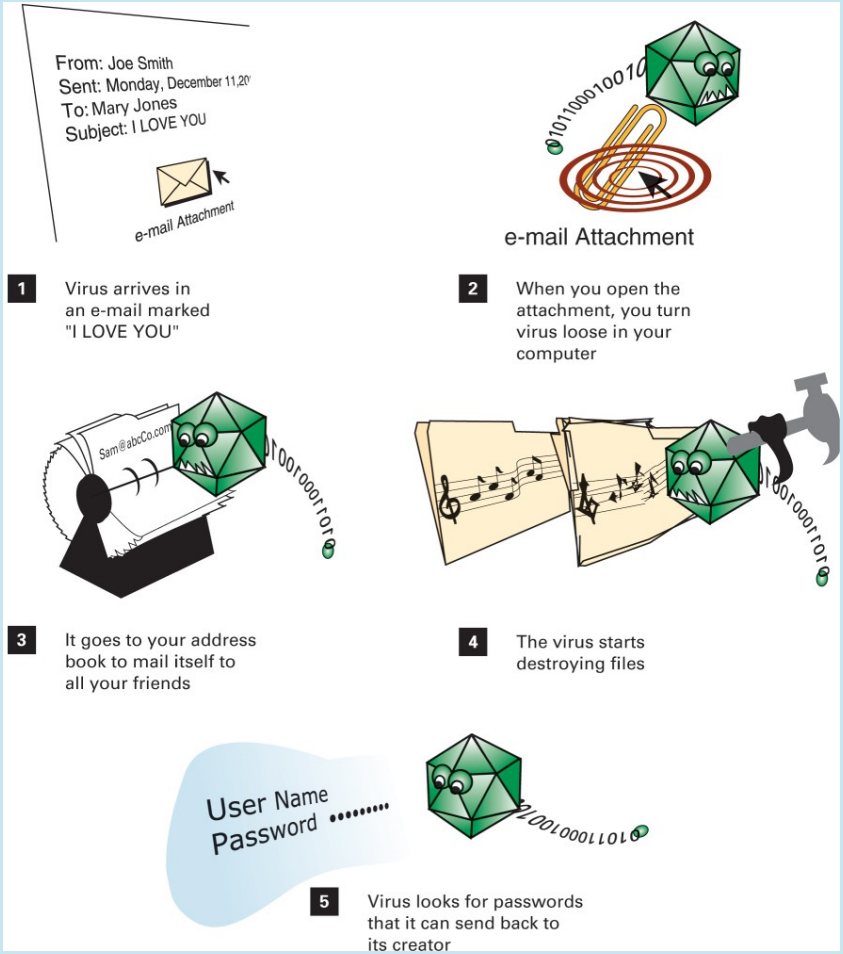
Types of Malware

- Malware – software designed to harm you computer or computer security
  - Viruses
  - Worms
  - Misleading e-mail
- Types of Malware
  - Denial-of-service attacks
  - Web defacing
  - Malware bots

Viruses

- ***Computer virus (virus)*** – software that was written with malicious intent to cause annoyance or damage
- ***Worm*** – a computer virus that replicates and spreads itself from computer to computer

The Love Bug Worm



Stand-Alone Viruses

- ***Spoofing*** – forging of return address on e-mail so that it appears to come from someone other than sender of record
- *Klez* family of worms
  - Introduced spoofing of sender and recipient

Trojan Horse Viruses

- ***Trojan horse virus*** – hides inside other software, usually an attachment or download
- Examples:
  - ***Key logger (key trapper) software*** – program that, when installed on a computer, records every keystroke and mouse click
  - Ping-of-Death DoS attack designed to crash Web sites

Misleading E-mail: Virus Hoax

- Objective is to cause damage to your system
- Virus hoax is an e-mail telling you of a non-existent virus
  - Makes recipients believe that they already have a virus and gives instructions on removal which actually delete a Windows file
  - Often purports to come from Microsoft -Microsoft always sends you to a Web site to find the solution to such a problem

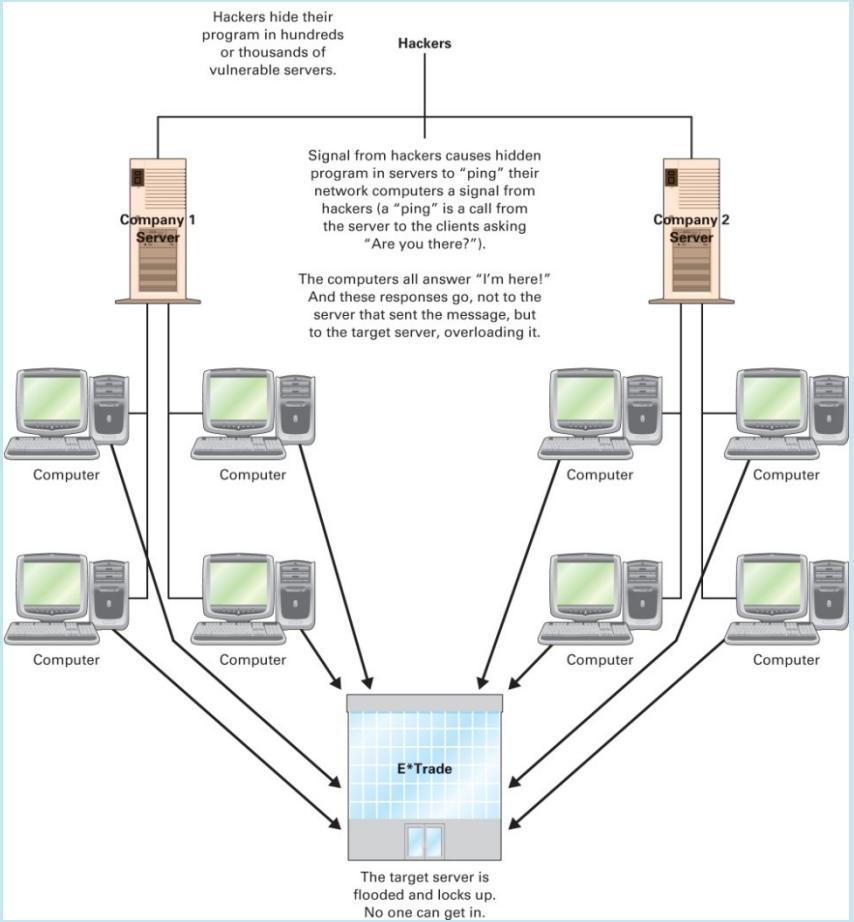
Denial-of-Service Attacks

- ***Denial-of-Service (DoS) attack*** – floods a Web site with so many requests for service that it slows down or crashes
- Objective is to prevent legitimate customers from using Web site

Distributed DoS

- ***Distributed denial-of-service attack (DDoS)*** – attacks from multiple computers that flood a Web site with so many requests for service that it slows down or crashes.

Distributed Denial-of-Service Attack



Malware Bots

- ***Bot*** – a computer program that runs automatically.
- ***Malware bots*** – bots that are used for fraud, sabotage, denial-of-service attacks, or some other malicious purpose
- ***Zombies (or drones)*** – malware-bot-infected computers

Botnets and Rootkits

- ***Botnet*** – a network of malware-bot infected computers
- ***Rootkit*** – software that gives you administrator rights to a computer or network and whose purpose is to allow you to conceal processes, files, or system data from the operating system

Web Defacing

- ***Web defacing*** – maliciously changing another's Web site
- Electronic equivalent of graffiti

Players

- ***Hackers*** – knowledgeable computer users who use their knowledge to invade other people's computers
- ***Thrill-seeker hackers*** – break into computer systems for entertainment
- ***White-hat (ethical) hackers*** – computer security professionals who are hired by a company to uncover vulnerabilities in a network

Players

- ***Black hat hackers*** – cyber vandals. They're the people who exploit or destroy information
- ***Crackers*** – hackers for hire, are the people who engage in electronic corporate espionage
  - ***Social engineering*** – acquiring information that you have no right to by means of deception

Players

- ***Hacktivists –*** politically motivated hackers who use the Internet to send a political message
- ***Cyberterrorists*** – those who seek to cause harm to people or destroy critical systems or information

Players

- ***Script kiddies (or bunnies)*** – people who would like to be hackers but don't have much technical expertise
  - Are often used by experienced hackers as shields

DIGITAL FORENSICS

- ***Digital forensics*** – the collection, authentication, preservation, and examination of electronic information for presentation in court
- Two phases
  1. Collecting, authenticating, and preserving electronic evidence
  2. Analyzing the findings

Phase 1: Collection – Places to look for Electronic Evidence

- Floppy disks
- CDs
- DVDs
- PDAs
- USB drives
- Flash memory cards, like an xD-Picture card, CompactFlash card, or similar storage medium for digital cameras and other devices
- Backup tapes of other media
- USB mass storage devices such as Thumb drives
- Voice mail
- Cell phones
- Electronic calendars
- MP3 players and IPods
- Scanner
- Pocket PCs
- Photocopiers
- Fax machines

Phase 1: Preservation

- If possible, hard disk is removed without turning computer on
- Special forensics computer is used to ensure that nothing is written to drive
- ***Forensic image copy*** – an exact copy or snapshot of all stored information

Phase 1: Authentication

- Authentication process necessary for ensuring that no evidence was planted or destroyed
- ***MD5 hash value*** – mathematically generated string of 32 letters and is unique for an individual storage medium at a specific point in time
  - Probability of two storage media having same MD5 hash value is 1 in 10^{38}, or
    - 1 in 100,000,000,000,000,000,000,000,000,000,000,000

Forensic Hardware and Software Tools

- Forensics computers usually have a lot of RAM and very fast processors
- EnCase – software that finds all information on disks
- Quick View Plus and Conversions Plus – read files in many formats
- Mailbag Assistant – reads most e-mail

Forensics Hardware and Software Tools

- Gargoyle – software that identifies encrypted files and may decrypt them
- Irfan View – reads image files
- Ingenium – semantic analysis software that searches for meaning rather than an exact match

Cell Phones

- In 2004 - 200 countries with more than 1.5 billion users of GSM cell phones (Cingular and most of Europe)
- Cell phones can be used for
  - Illegal drug deals
  - Storing stolen data
  - Fraudulently securing goods and services
  - Setting off explosives

Cell Phones and Other Handheld Devices Files Can Be Recovered from…

- Phone book
- Subscriber, equipment, and service provider identifiers
- Calendar
- To-Do list
- Phone number log and most recently dialed numbers
- E-mail
- Web activity
- Text messages and multimedia messages
- Voice mail
- Electronic documents
- Last active location and other networks encountered
- Graphics, photos and videos

Phase 2: Analysis

- Interpretation of information uncovered
- Recovered information must be put into context
- Digital forensic software pinpoints the file's location on the disk, its creator, the date it was created and many other features of the file

Where Data is Hiding

E-Mail Files
• E-mail messages
• Deleted e-mail messages
Program Files and Data Files
• Word (.doc) and backup (.wbk) files
• Excel files
• Deleted files of all kinds
• Files hidden in image and music files
• Encrypted files (with keys or passwords)
• Compressed files
Web Activity Files
• Web history
• Cache files
• Cookies
Network Server Files
• Backup e-mail files
• Other backup and archived files
• System history files
• Web log files

History of Disk Activity

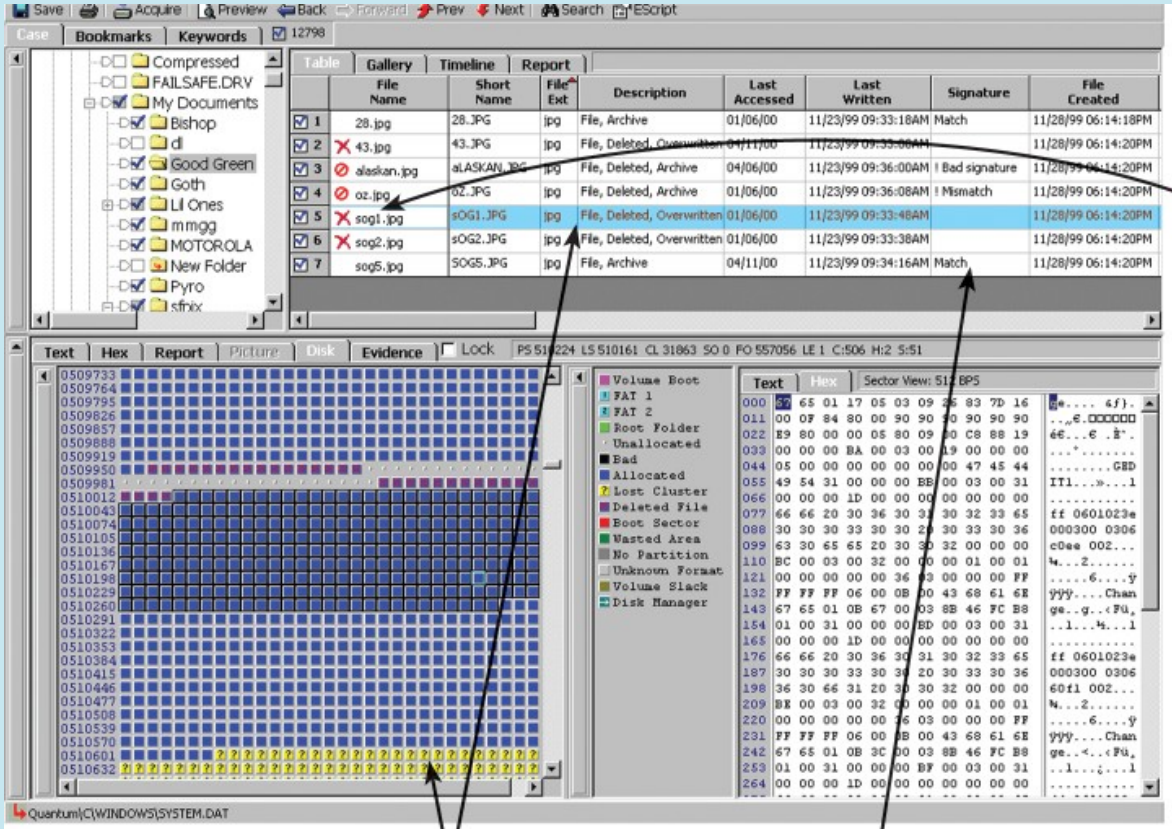


Figure H.9

History of File Activity

File marked as deleted

Details of where files are located on the disk, whether they've been deleted, overwritten, or archived

Information on whether the contents matches the extension or not

Live Analysis

- Examination of a system while it is still running
- Disadvantage - not possible to get an MD5 hash value
- Advantages include – the ability to retrieve information from RAM
- Helix – program to collect information during live analysis

RECOVERY AND INTERPRETATION

- Snippets of e-mail, when put into context, often tell an interesting story

E-Mail between engineers about the Spaceship Columbia

" . . . something could get screwed up enough . . . and then you are in a world of hurt . . . "

and

"I can only hope the folks . . . are listening . . . "

E-Mail between Enron and Andersen Consulting

To: David B. Duncan
Cc: Michael C. Odom@ANDERSEN WO: Richard Corgci@ANDERSEN WO
BCC:
Date: 10/16/2001 08:39 PM
From: Nancy A. Temple
Subject: Re: Press Release draft
Attachments: ATT&ICIQ: 3rd qtr press release memo.doc

Dave - Here are a few suggested comments for consideration.

- I recommend deleting reference to consultation with the legal group and deleting my name on the memo. Reference to the legal group consultation arguably is a waiver of attorney-client privileged advice and if my name is mentioned it increases the chances that I might be a witness, which I prefer to avoid.

- I suggested deleting some language that might suggest we have concluded the release is misleading.

- In light of the "non-recurring" characterization, the lack of any suggestion that this characterization is not in accordance with GAAP, and the lack of income statements in accordance with GAAP, I will consult further within the legal group as to whether we should do anything more to protect ourselves from potential Section 10A issues.

E-Mail from Arresting Officer in the Rodney King Beating

"oops I haven't beaten anyone so bad in a long time...."

Internal E-Mail from Bill Gates to Microsoft Employee

" . . . do we have a clear plan on what we want Apple to do to undermine Sun . . . ?"

Places to Look for Useful Information

- Deleted files and slack space
  - ***Slack space*** – the space between the end of the file and the end of the cluster
- System and registry files
  - Controls virtual memory on hard disk
  - Has records on installs and uninstalls
  - Has MAC address (unique address of computer on the network)

Places to Look for Useful Information

- ***Unallocated space*** – set of clusters that has been marked as available to store information but has not yet received any
- Unused disk space
- Erased information that has not been overwritten

Anti-Forensics

- New branch of digital forensics
- Set of tools and activities that make it hard or impossible to track user activity
- Three categories
  - Configuration settings
  - Third party tools
  - Forensic defeating software

Configuration Settings Examples:

- Use *Shift* + *Delete* to bypass the recycle bin
- Rename the file with a different extension
- Clear out virtual memory
- Use *Defrag* to rearrange data on the hard disk and overwrite deleted files
- Use *Disk Cleanup* to delete ActiveX controls and Java applets

Configuration Settings Examples:

- Delete temporary Internet files
- Hide information by making it invisible with *Hidden* feature in Word or Excel
- ***Redact*** – black out portions of a document
- Protect your files with passwords

Configuration Settings Examples:

- Make the information invisible
- Use Windows to hide files
- Protect file with password

Third-Party Tools to

- Alter your registry
- Hide Excel files inside Word documents and visa versa
- Change the properties like creation date in Windows
- Replace disk contents with 1’s and 0’s – called wiping programs

Third Party Tools

- ***Encryption*** – scrambles the contents of a file so that you can't read it without the decryption key
- ***Steganography*** – hiding information inside other information
  - The watermark on dollar bills is an example
- ***U3 Smart drive*** – stores and can launch and run software without going through the hard disk thus leaving no trace of itself

Forensic Defeating Software

- Software on the market specially designed to evade forensic examination
- Such software would include programs to remove
  - data in slack space
  - data in cache memory
  - cookies, Internet files, Google search history, etc.

WHO NEEDS DIGITAL FORENSICS INVESTIGATORS?

- Digital forensics is used in
  - The military for national and international investigations
  - Law enforcement, to gather electronic evidence in criminal investigations
  - Corporations and not-for-profits for internal investigations
  - Consulting firms that special in forensics

Organizations Use Digital Forensics in Two Ways

1. Proactive education to educate employees
2. Reactive digital forensics for incident response

Proactive Education to Educate Employees

- Proactive Education for Problem Prevention
  - What to do and not to do with computer resources such as
    - The purposes for which e-mail should be used
    - How long it may be saved
    - What Internet sites are may be visited

Reactive Digital forensics for Incident Response

- What to do if wrong-doing is suspected and how to investigate it
  - Encouraged by the Sarbanes-Oxley Act, which expressly requires implementation of policies to prevent illegal activity and to investigate allegations promptly

A Day in the Life…

- As a digital forensics expert you must
  - Know a lot about computers and how they work
  - Keep learning
  - Have infinite patience
  - Be detail-oriented
  - Be good at explaining how computers work
  - Be able to stay cool and think on your feet