CYBERSPACE AND CRIMINAL BEHAVIOR

CYBERSPACE

- Cyberspace refers to the virtual space that provides the infrastructure, electronic medium and related elements necessary for online global communication.
- It can be thought of as the second life space where human beings operate for social interactions, entertainment, business operations as well as for personal activities and interests.
- The term cyberspace is derived from the word cybernetics which in turn is extracted from ancient Greek word kubernētēs, that refers to steersman or to give direction.
- The term cyberspace first came into existence in various contexts in visual arts and science fiction during 1940, 1960 and 1984.
- However, the first reference was made by the founder of Electronic Frontier Foundation, in the year 1990 and later in 1991 by Mr. Benedict, which is close to the existing relationship of computer and telecommunication systems.
- The virtual library of information offers required information on any topic at any point of time and cyberspace acts as the informational resource now-a-days. Entertainment and social networking play a major role in cyberspace as the cyberspace has been evolving as a great medium to connect people these days.

THE ADVANTAGES OF CYBERSPACE INCLUDE

- Informational resources
- Entertainment
- Social networking

DISADVANTAGE

- The disadvantages are due to this great medium of connectivity, as it leads to spamming, theft of information and threats etc.
- A cybercriminal is an individual who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both.
- Cybercriminals tries to use the computers in three broad ways. Firstly, they use the computer as their target for attacking other people's computers for the purpose of fulfilling their malicious activities like spreading viruses, data theft, identity theft, etc.
- Secondly, they use the computer as their weapon for the purpose of carrying out conventional crime like spam, fraud, illegal gambling, etc.
- Thirdly, they use the computer as their accessory for the purpose of saving stolen or illegal data.Thus cyberspace provides a platform for all criminal activities and therefore, security is a major challenge.

TRADITIONAL PROBLEMS ASSOCIATED WITH COMPUTER CRIME

- Physicality and Jurisdictional Concerns
- Perceived Insignificance, Stereotypes, and Incompetence
- Prosecutorial Reluctance
- Lack of Reporting
- Lack of Resources
- Jurisprudential Inconsistency

PHYSICALITY AND JURISDICTIONAL CONCERNS

- Individuals sitting at their desk can enter various countries without the use of passports or documentation.
- For successful prosecution it is necessary to get the specification of the crime scene i.e.,
  - 1. Where did the crime actually occur?
  - 2. Which laws apply?
  - 3. Which agency is responsible for the investigation of a particular incident?
  - 4. Which agency has primary jurisdiction over the thief?

DIGITAL FORENSICS

- **The process of identifying preserving, analyzing and presenting digital evidence for a legal proceeding**

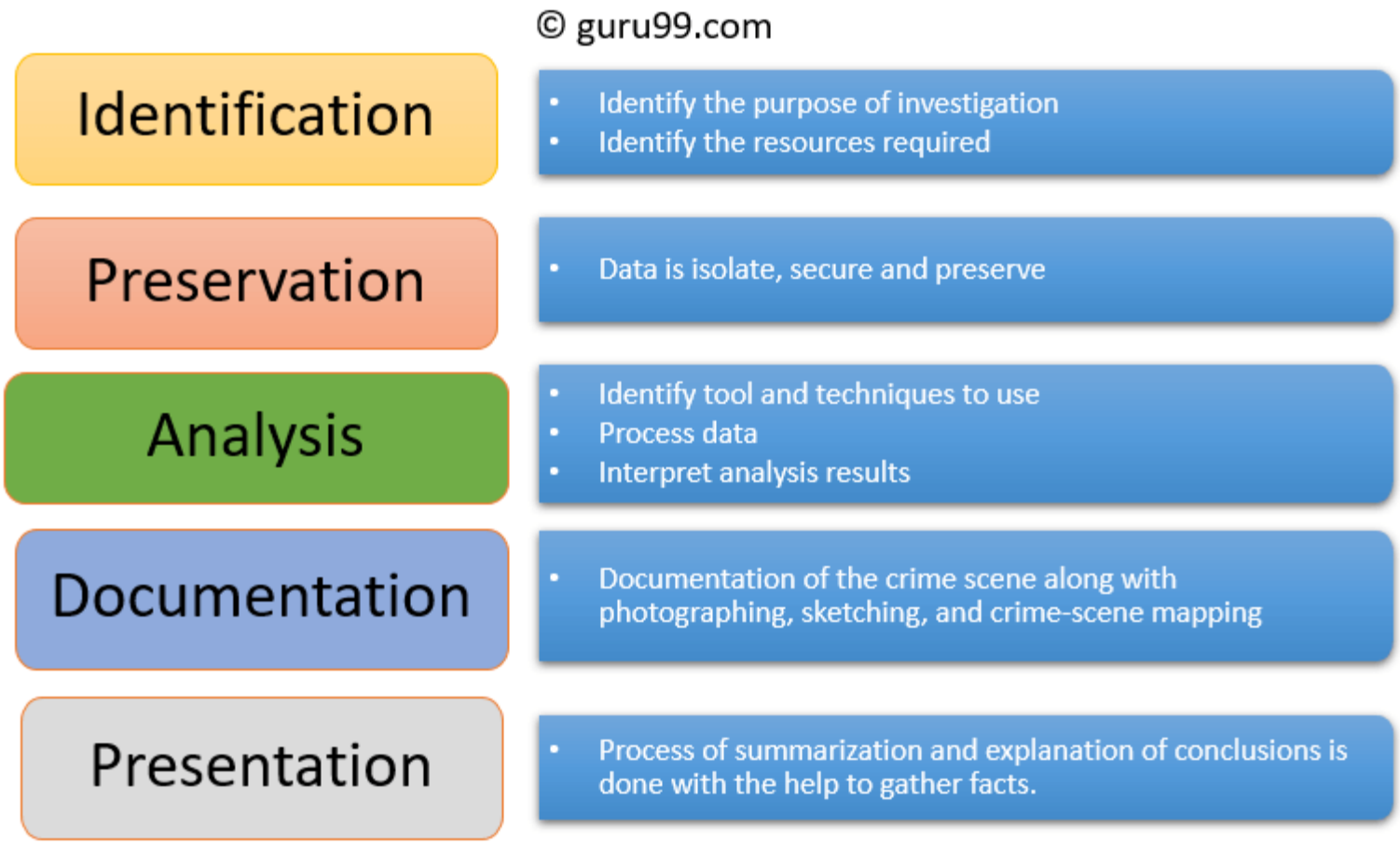
DIGITAL FORENSICS

- Digital Forensics is the preservation, identification, extraction, interpretation and documentation of computer evidence which can be used in the court of law. Technically, the term computer forensics refers to the investigation of computers. Digital forensics includes not only computers but also any digital device, such as digital networks, cellphones, flash drives and digital cameras.

PROCESS OF DIGITAL FORENSICS

- Digital forensics entails the following steps:
  - Identification
  - Preservation
  - Analysis
  - Documentation
  - Presentation
-

PROCESS


© guru99.com
Identification
Identify the purpose of investigation
Identify the resources required
Preservation
Data is isolate, secure and preserve
Analysis
Identify tool and techniques to use
Process data
Interpret analysis results
Documentation
Documentation of the crime scene along with photographing, sketching, and crime-scene mapping
Presentation
Process of summarization and explanation of conclusions is done with the help to gather facts.

TYPES OF DIGITAL FORENSICS

- Disk Forensics
- Network Forensics
- Wireless Forensics
- Database Forensics
- Malware Forensics
- Malware Forensics
- Memory Forensics
- Mobile Phone Forensics

CHALLENGES FACED BY DIGITAL FORENSICS

- The increase of PC's and extensive use of internet access
- Easy availability of hacking tools
- Lack of physical evidence makes prosecution difficult.
- The large amount of storage space into Terabytes that makes this investigation job difficult.
- Any technological changes require an upgrade or changes to solutions.

EXAMPLE USES OF DIGITAL FORENSICS

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Inappropriate use of the Internet and email in the workplace
- Forgeries related matters
- Bankruptcy investigations
- Issues concern with the regulatory compliance

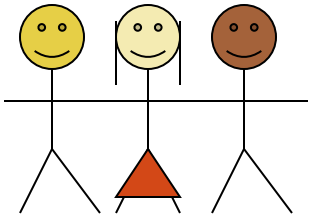
ADVANTAGES OF DIGITAL FORENSICS

- To ensure the integrity of the computer system.
- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies to capture important information if their computer systems or networks are compromised.
- Efficiently tracks down cybercriminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

DISADVANTAGES OF DIGITAL FORENSICS

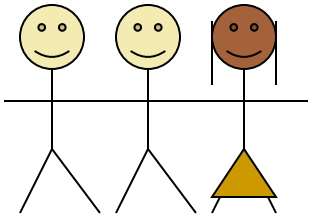
- Digital evidence accepted into court. However, it is must be proved that there is no tampering
- Producing electronic records and storing them is an extremely costly affair
- Legal practitioners must have extensive computer knowledge
- Need to produce authentic and convincing evidence
- If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
- Lack of technical knowledge by the investigating officer might not offer the desired result

DIFFERENCE



IMT: Incident Management Team

IS Mgr leads, includes steering committee, IRT members
Develop strategies & design plan for Incident Response, integrating business, IT, BCP, and risk management
Obtain funding, Review postmortems
Meet performance & reporting requirements

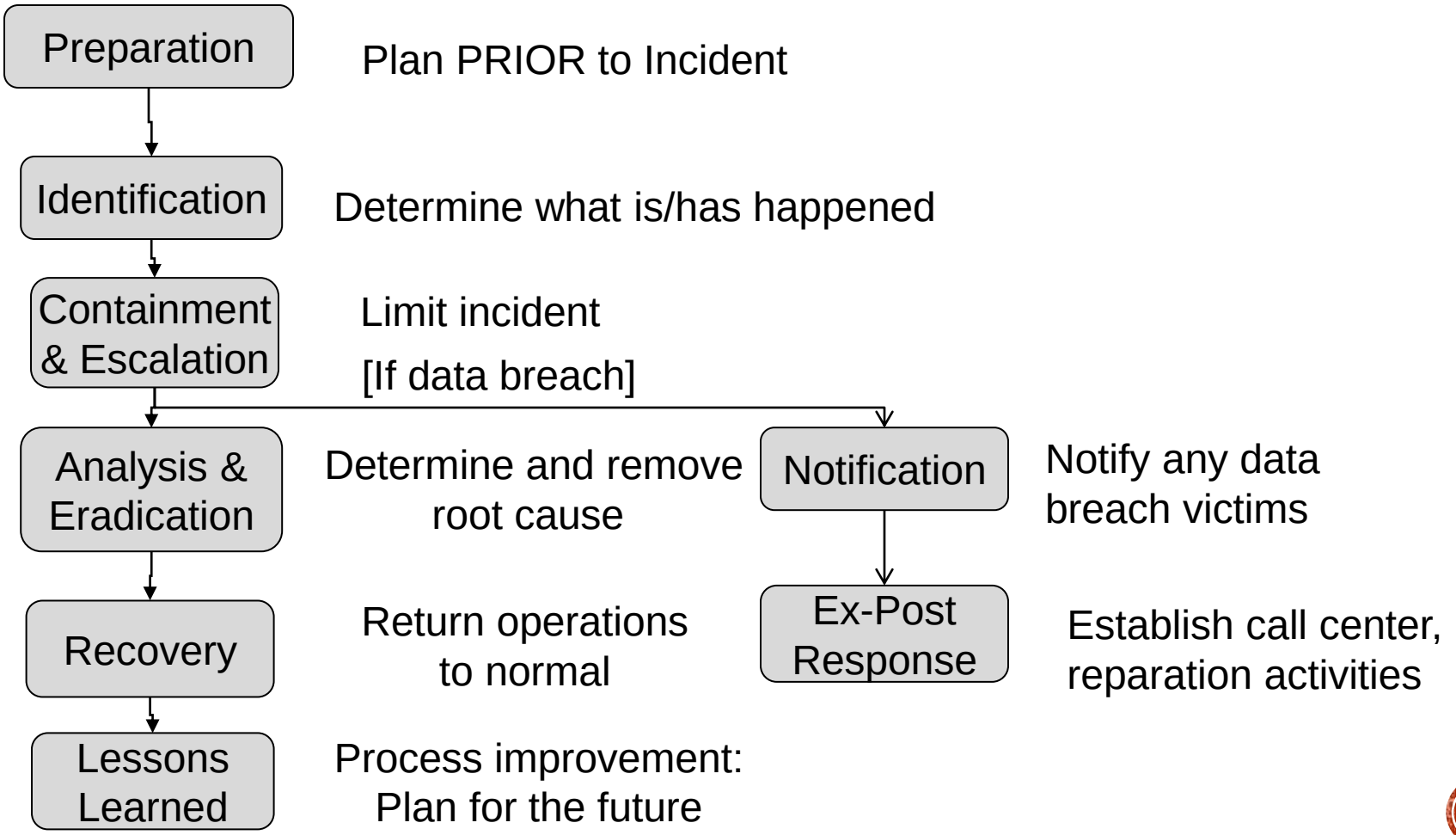


IRT: Incident Response Team

Handles the specific incident. Has specific knowledge relating to: Security, network protocols, operating systems, physical security issues, malicious code, etc.

Permanent (Full Time) Members: IT security specialists, incident handlers, investigator
Virtual (Part Time) Members: Business (middle mgmt), legal, public relations, human resources, physical security, risk, IT

STAGES IN INCIDENT RESPONSE



WHY IS INCIDENT RESPONSE IMPORTANT?

- Average Cost of Data Breach:
- Global $3.86M; U.S. $7.91M for 31,465 records
- Mega Breach: 1 M records: $40 million 50 M records: $350 million
- Mean Time to Identify (MTTI): Days to find, confirm breach
- Mean Time to Contain (MTTC): Days to resolve breach and restore service

	Global	U.S.	India	Criminal attack	System Glitch	Human Error
Mean Time to Identify	196.7	201	188	221	177	174
Mean Time to Contain	69.0	52	78	81	60	57

2018 Cost of a Data Breach Study: Global Report (IBM/Ponemon)

STAGE 1: PREPARATION

- What shall we do if different types of incidents occur? (BIA helps)
- When is the incident management team called?
- How can governmental agencies or law enforcement help?
- When do we involve law enforcement?
- What equipment do we need to handle an incident?
- What shall we do to prevent or discourage incidents from occurring? (e.g. banners, policies)
- Where on-site & off-site shall we keep the IRP?

(1) DETECTION TECHNOLOGIES

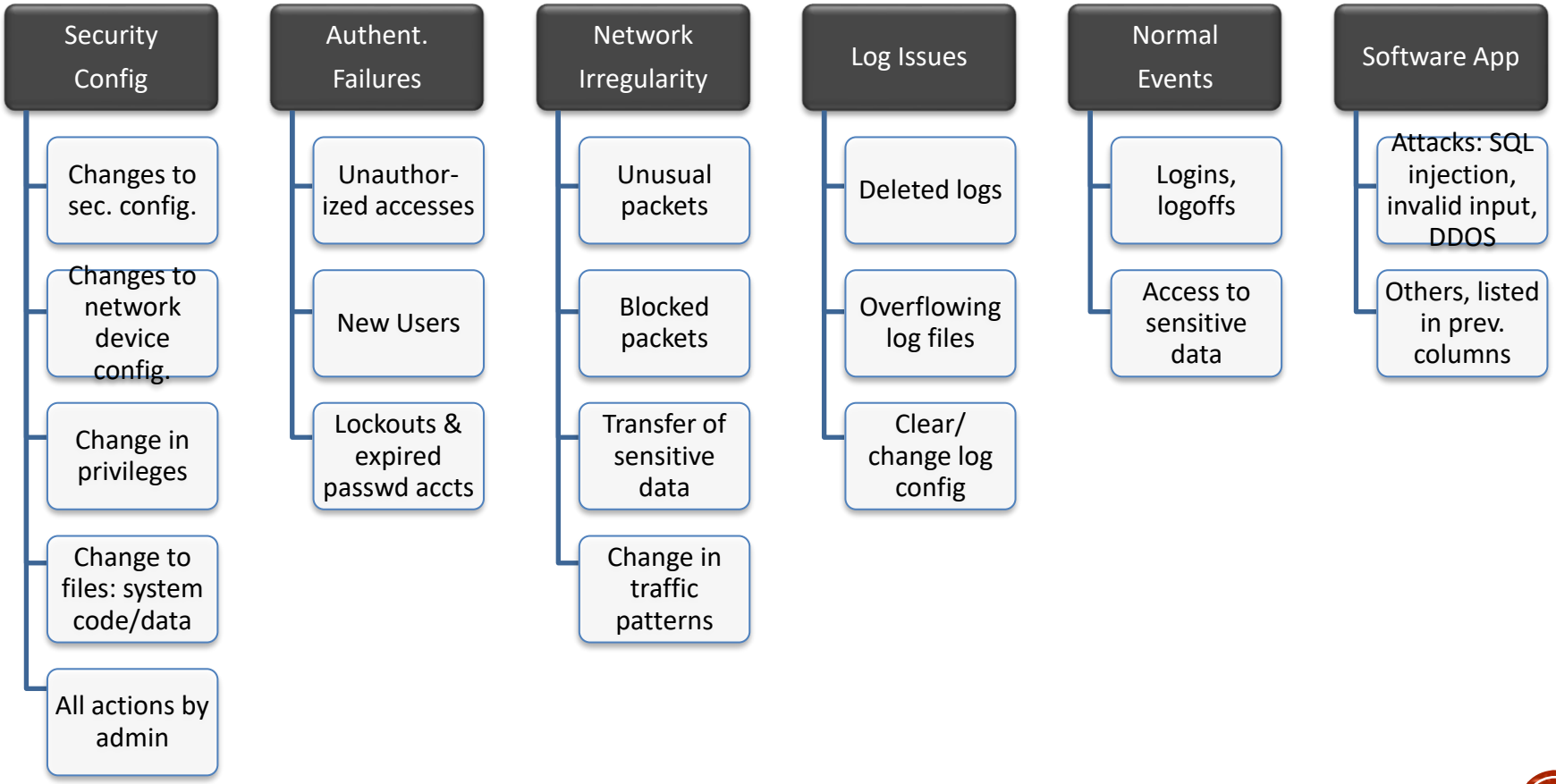
Organization must have sufficient detection & monitoring capabilities to detect incidents in a timely manner

Proactive Detection includes:

- Network Intrusion Detection/Prevention System (NIDS/NIPS)
- Host Intrusion Detection/Prevention System (HIDS/HIPS)
- Antivirus, Endpoint Security Suite
- Security Information and Event Management (Logs)
- Vulnerability/audit testing
- System Baselines, Sniffer
- Centralized Incident Management System
  - Input: Server, system logs
  - Coordinates & co-relates logs from many systems
  - Tracks status of incidents to closure

Reactive Detection: Reports of unusual or suspicious activity

LOGS TO COLLECT & MONITOR



INCIDENTS MAY INCLUDE…

IT Detects

- a device (firewall, router or server) issues serious alarm(s)
- change in configuration
- an IDS/IPS recognizes an irregular pattern:
  - unusually high traffic,
  - inappropriate file transfer
  - changes in protocol use
- unexplained system crashes or
- unexplained connection terminations

Employees Reports

- Malware
- Violations of policy
- Data breach:
  - stolen laptop, memory
  - employee mistake
- Social engineering/fraud:
  - caller, e-mail, visitors
- Unusual event:
  - inappropriate login
  - unusual system aborts
  - server slow
  - deleted files
  - defaced website

(1) MANAGEMENT PARTICIPATION

- Management makes final decision
  - As always, senior management has to be convinced that this is worth the money.
- Actual Costs: Cost of a Data Breach Study, 2018, Ponemon, IBM

Expenses Following a Breach	Average Cost (U.S.)
Detection and Escalation: forensic investigation, audit, crisis mgmt., board of directors involvement	**$1,210,000**
Notification: legal expertise, contact database development, customer communications	**$740,000**
Post Breach Response: help desk and incoming communications, identity protection services, legal and regulatory expenses, special investigations	**$1,760,000**
Lost Business: abnormal customer churn, customer procurement, goodwill	**$4,200,000**

WORKBOOK
INCIDENT TYPES

Incident	Description	Methods of Detection	Procedural Response
Intruder accesses internal network	Firewall, database, IDS, or server log indicates a probable intrusion.	Daily log evaluations, high priority email alerts	IT/Security addresses incident within 1 hour: Follow: Network Incident Procedure Section.
Break-in or theft	Computers, laptops or memory is stolen or lost.	Security alarm set for off-hours; or employee reports missing device.	Email/call Management & IT immediately. Management calls police, if theft. Security initiates tracing of laptops via location software, writes Incident Report, evaluates if breach occurred.
Social Engineering	Suspicious social engineering attempt was recognized OR information was divulged that was recognized after the fact as being inappropriate.	Training of staff leads to report from staff	Report to Management & Security. Warn employees of attempt as added training. Security evaluates if breach occurred, writes incident report.
Trojan Wireless LAN	A new WLAN masquerades as us.	Key confidential areas are inspected daily for WLAN availability	Security or network administrator is notified immediately. Incident is acted upon within 2 hours.

STAGE 2: IDENTIFICATION

Triage: Categorize, prioritize and assign events and incidents

- What type of incident just occurred?
- What is the severity of the incident?
  - Severity may increase if recovery is delayed
- Who should be called?
- Establish chain of custody for evidence

(2) TRIAGE

Snapshot of the known status of all reported incident activity

- Sort, Categorize, Correlate, Prioritize & Assign

Categorize: DoS, Malicious code, Unauthorized access, Inappropriate usage, Multiple components

Prioritize: Limited resources requires prioritizing response to minimize impact

Assign: Who is free/on duty, competent in this area?

(2) CHAIN OF CUSTODY

- Evidence must follow Chain of Custody law to be admissible/acceptable in court
- Include: specially trained staff, 3rd party specialist, law enforcement, security response team

System administrator can:

- Retrieve info to confirm an incident
- Identify scope and size of affected environment (system/network)
- Determine degree of loss/alteration/damage
- Identify possible path of attack

STAGE 3: CONTAINMENT

- Activate Incident Response Team to contain threat
  - IT/security, public relations, mgmt, business
- Isolate the problem
  - Disable server or network zone comm.
  - Disable user access
  - Change firewall configurations to halt connection
- Obtain & preserve evidence

(3) CONTAINMENT - RESPONSE

Technical

- Collect data
- Analyze log files
- Obtain further technical assistance
- Deploy patches & workarounds

Managerial

- Business impacts result in mgmt intervention, notification, escalation, approval

Legal

- Issues related to: investigation, prosecution, liability, privacy, laws & regulation, nondisclosure

STAGE 4: ANALYSIS & ERADICATION

- Determine how the attack occurred: who, when, how, and why?
  - What is impact & threat? What damage occurred?
- Remove root cause: initial vulnerability(s)
  - Rebuild System
  - Talk to ISP to get more information
  - Perform vulnerability analysis
  - Improve defenses with enhanced protection techniques
- Discuss recovery with management, who must make decisions on handling affecting other areas of business

(4) ANALYSIS

- What happened?
- Who was involved?
- What was the reason for the attack?
- Where did attack originate from?
- When did the initial attack occur?
- How did it happen?
- What vulnerability enabled the attack?

(4) REMOVE ROOT CAUSE

- If Admin or Root compromised, rebuild system
- Implement recent patches & recent antivirus
- Fortify defenses with enhanced security controls
- Change all passwords
- Retest with vulnerability analysis tools

STAGE 5: RECOVERY

- Restore operations to normal
- Ensure that restore is fully tested and operational

WORKBOOK
INCIDENT HANDLING RESPONSE

Incident Type: Malware detected by Antivirus software
Contact Name & Information: Computer Technology Services Desk: www.univ.edu/CTS/help 262-252-3344(O)
Emergency Triage Procedure: Disconnect computer from Internet/WLAN. Do not reconnect. Allow anti-virus to fix problem, if possible. Report to IT first thing during next business day.
Containment & Escalation Conditions and Steps: If laptop contained confidential information, investigate malware to determine if intruder obtained entry. Determine if Breach Law applies.
Analysis & Eradication Procedure: If confidential information was on the computer (even though encrypted), malware may have sent sensitive data across the internet; A forensic investigation is required. Next, determine if virus=dangerous and user=admin: Type A: return computer. (A=Virus not dangerous and user not admin.) Type B: Rebuild computer. (B=Either virus was dangerous and/or user was admin) Password is changed for all users on the computer.
Other Notes (Prevention techniques): Note: Antivirus should record type of malware to log system.

STAGE 6: LESSONS LEARNED

- **Follow-up includes:**
- Writing an Incident Report
  - What went right or wrong in the incident response?
  - How can process improvement occur?
  - How much did the incident cost (in loss & handling & time)
- Present report to relevant stakeholders

COMPUTER LANGUAGE

- Computers are the mechanism through which raw information (i.e., data) is processed.
- Although raw data may seem complex to understand, the structure of data is actually very basic, and is based on a binary language.
- The smallest piece of data is called a bit.
- Each bit has two possible electrical states, on (1) or off (0).
- Thus, raw data is a series of 1s and 0s. Of course, raw data is difficult to interpret by users, so computers group bits together to provide identifiable meaning.
- The smallest such grouping occurs when eight bits are combined to form a byte.
- Each byte of data represents a letter, number, or character. For example, the raw data sequence of 01000001 appears to the user as the capital letter "A."
- As stored information has increased, the data capacity of computers is also increased from kilobytes (KB) to megabytes (MB) to gigabytes (GB), and now, terabytes (TB).

NETWORK LANGUAGE

- TCP/IP
- IMAP
- POP
- Routers
- Hubs
- Packets
- Cookies
- DNS

TCP/IP

- TCP/IP stands for Transmission Control Protocol/Internet Protocol.
- It refers to the suite of protocols that define the Internet.
- TCP is a method of communication between programs which enables a bit-stream transfer of information.
- Originally proposed and designed as the standard protocol for ARPANet, but now TCP/IP software is available for every major kind of computer operating system.
- Luckily, it is now built into many of the most common operating systems.

IMAP

- IMAP stands for Internet Message Access Protocol.
- It is an internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection.
- E-mail stored on an IMAP server can be manipulated from anywhere without the need to transfer messages or files back and forth between the computers.

POP

- POP stands for Post Office Protocol. Post Office Protocol is a standard mail protocol used to receive emails from a remote server to a local email client.
- It allows you to download email messages on your local computer and read them even when you are offline.
- It was designed to support offline/local email processing.
- Once the messages are downloaded, they are deleted from the mail server.
- This mode of access is not compatible with access from multiple computers.

ROUTERS

- Routers are defined as special-purpose computers that handle the connection between two or more networks.
- Routers spend all their time looking at the destination addresses of the packets passing through them and deciding which route to send them on.

HUB

- Hub is used for connecting multiple computers or segments of a LAN.
- Hubs are central switching devices for communications lines in a star topology.
- Hubs may be added to bus topologies, for example, a hub can turn an Ethernet network into a star topology to improve troubleshooting.

PACKETS

- Packets are the basic units of communication over a TCP/IP network.
- They are defined as units of data exchanged between host computers.
- A packet is a string of bits divided into three main sections:
  - 1. A set of headers
  - 2. The payload, the actual data being transmitted
  - 3. The trailer, sometimes called the footer
- Packet switching refers to the method used to move data around on the Internet. In packet switching, all the data coming out of a machine are broken up into chunks; each chunk has the address of where it came from and where it is going

COOKIES

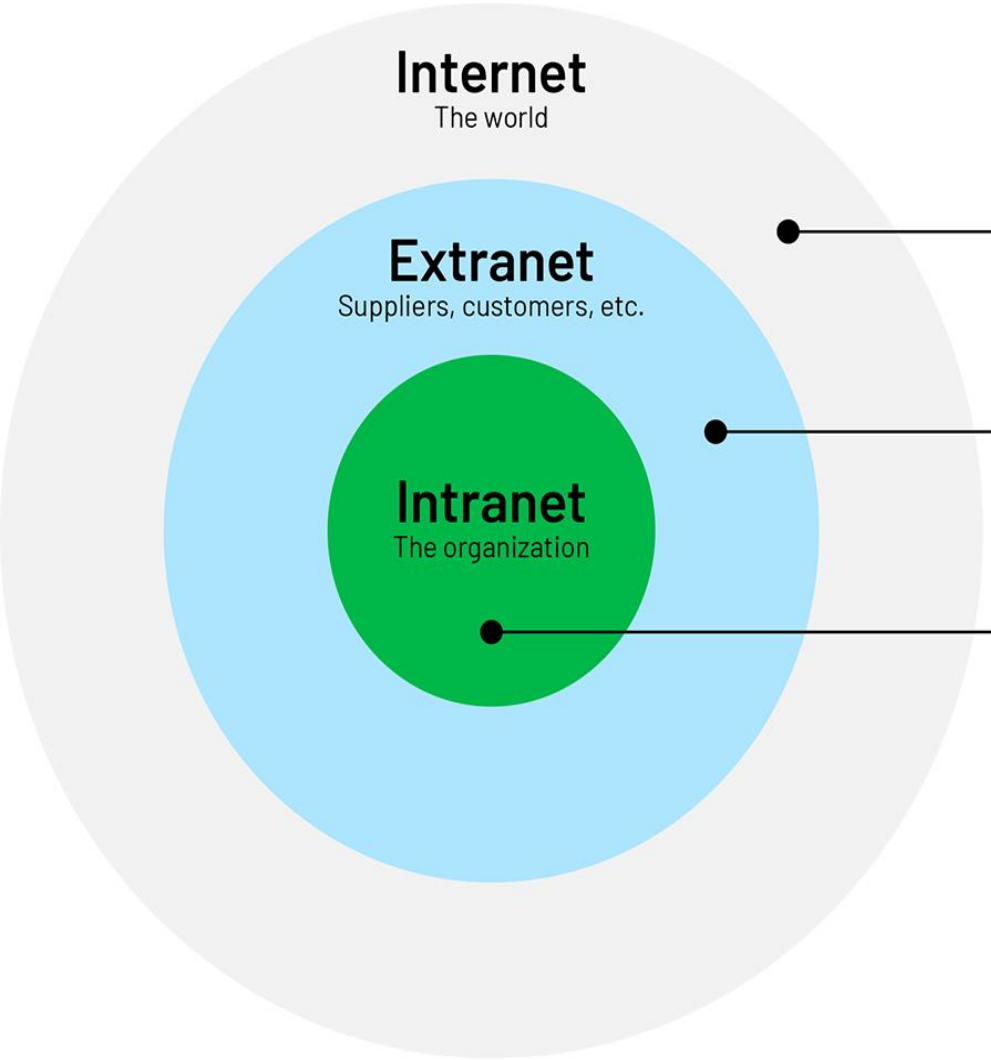
- Cookies are small pieces of information that an HTTP server sends to the individual browser upon the initial connection.
- Not all browsers support cookies. However, most popular browsers such as MS Internet Explorer 3.0 or higher and Netscape Navigator 2.0 and higher.
- Cookies might contain information such as login or registration information, online "shopping cart" information, user preferences, and so on.
- When a server receives a request from a browser that includes a cookie, the server is able to use the information stored in the cookie.
- Cookies do not steal information. They simply act as storage platforms for information that a user has supplied.

DNS

- DNS stands for Domain Name System.
- Domain Name System is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.
- DNS eases the translation of IP addresses through the utilization of hierarchical principles.
- Traditional top-level domain names include com (commercial organization), edu (educational institutions), gov (government organizations), org (nonprofit organizations), and net (Internet access providers).

REALMS OF THE CYBER WORLD

- Intranets
- Extranet
- The Internet



The **internet** creates connections between computers around the world.

An **extranet** creates connections beyond (or outside) an organization.

An **intranet** creates connections inside an organization.

CONT …

- There are three different levels of networked systems: intranets, internets, and the Internet.
- **Intranets** are small local networks connecting computers which are within one organization and which are controlled by a common system administrator.
- **Internets**, on the other hand, connect several networks, and are distinguished in the literature by a lower case i (i.e., “internet” as opposed to “Internet”). These networks are usually located in a small geographic area, and share a common protocol (usually TCP/IP).
- **The Internet**, on the other hand, is the largest network in the world, an international connection of all types and sizes of computer systems and networks. It is a system of small networks of computers linked with other networks via routers and software protocols.
- This TCP/IP based network links tens of millions of users, across more than 45,000 networks, in countries spanning the globe. The Internet has become the backbone for global communications and transnational capitalism. •
- During the Internet’s infancy, users could connect only via standardized modems and telephone lines.

CONT …

- Early service providers, like AOL, initially charged users for the period of time they spent on the Internet. As connection speeds via modems were notoriously slow, individuals racked up substantial charges. This expense was compounded by users who connected via long-distance numbers.
- As a result, telephone companies became victimized by criminals (i.e., phreakers) seeking to avoid such charges. As competition increased with the birth of the “Baby Bells,” cost to consumers began to decline.
- Connections made via modem are known as dial-up connections. • Such connections were originally categorized by the transfer rate of data using an older measure of bandwidth known as baud.
- Initially, a transfer rate of 300 baud was common.
- Such rates quickly evolved as market demand increased, and 1,200, 2,400, 4,800, and 9,600 baud became the standard.
- As these modem bandwidth rates grew, a new designation of transfer speed was developed. Currently, data transfer rates are categorized as kilobits per second (Kbps) or megabits per second (Mbps).

THANK YOU