I.C.P.A.K ANNUAL FORENSIC AUDIT SEMINAR-

CYBER FRAUD

BY NASUMBA.K. KWATUKHA

C.P.A, C.I.A, C.F.E, C.I.S.A, C.I.S.S.P, C.R.M.A

EAST AFRICA

ELECTRONIC TRANSFERS

E - COMMERCE

THE DIGITAL GENERATION

- The internet in Kenya is growing rapidly. It has given rise to new opportunities in every field we can think of— be it politics-voting process, business processes and education. Tools include Computers and internet enabled devices such as mobile phones.
- Even dating and getting a wife and paying dowry

- The higher the levels of dependency and complexity of systems, the higher cyber frauds and complex the tools of a fraudster.

HOW DOES THE INTERNET WORK?

- Type URL :-www.kemu.com

.com-root server

- .Kemu-Name of the company

www-host name of the server

- URL loads using a certain path.

CYBER CRIMES

Defining Cyber Fraud

- Any embezzlement or defalcation accomplished by tampering with computer programs resulting in losses sustained by the organization, in which computer was manipulated.

- Specifically, cyber fraud involves the use of internet to perpetuate fraud.

CYBER FRAUD - REALITY IN KENYA

- Recognition of cyber fraud as one of the big five economic crimes in Kenya at 22% incidence reporting and what this means and why it could be higher- P.W.C economic crime report 2014.

- Victims in most cases do not know incidences of cyber fraud exe files, freeware, kindly sent a report.

- Cyber threat evolving with enhanced security mechanisms, and the changing face of social engineering

CHALLENGES IN THIS FIGHT

- Lack of traditional paper trails- error and event log trail.
- Require an understanding of technology used by the perpetrator.
- Technology of victim organization
- Specialized knowledge required
- Victim knowledge on what is happening it is not known

CATEGORIES OF CYBER CRIME

- We can categorize cyber crime in three ways:- from an investigative point of view
- The computer as a target :- Cyber fraud attacks target a computer e.g. Hacking, virus/worms attacks, Dos attack etc.
- The computer as a weapon :- using a computer to attack other computers or to commit real world crime e.g. credit card fraud and pornography etc.
- Computer as a symbol that lends credibility to the perpetrator.

- Cyber can also be used to modify and accelerate normal frauds; stealing of cash, gambling, robbery

- There those that depend wholly on the computer.

- Again, this is growing trend and it is surprising that authorities have not taken stern actions to curb the growth of these cyber-crimes.

- The police have recorded 3,038 cases but made only 2,700 arrests in 3 years (between 2007 and 2010)
- India registered only 1,350 cases under the IT Act and IPC in 2010
- 50% of cybercrimes are not even reported.

FREQUENTLY USED TECHNIQUES

Learning the target

- Name tags on officers; procedures of handling visitors;
- Social Engineering techniques such as confirmed M-pesa number;
- Sniffing packets and operating systems of victim-passwords;
- NMAP Port Scanning and response from network to initiate communication;
- Shoulder surfing; webpage error data; who is in find out.

WEB BASED EXPLOITS

- Hacking- Simple process of enumeration and Pen tests;
- URL Poisoning and web services query;
- WEB Poisoning and credit fraud; wrong passwords used.
- URL Exploits-wikileaks and D.P Ruto account;
- SQL Poisoning of the query machine; government hackers.

CONT'D OF ATTACKS

- HTTP mode; Cookies monitoring and review.

- Password crackers, random user password change and downloads;

- Remote Access Trojans :- exe, download latest, updates on Microsoft-complete charge of the system and install backdoors remotely.

-Hidden folders option

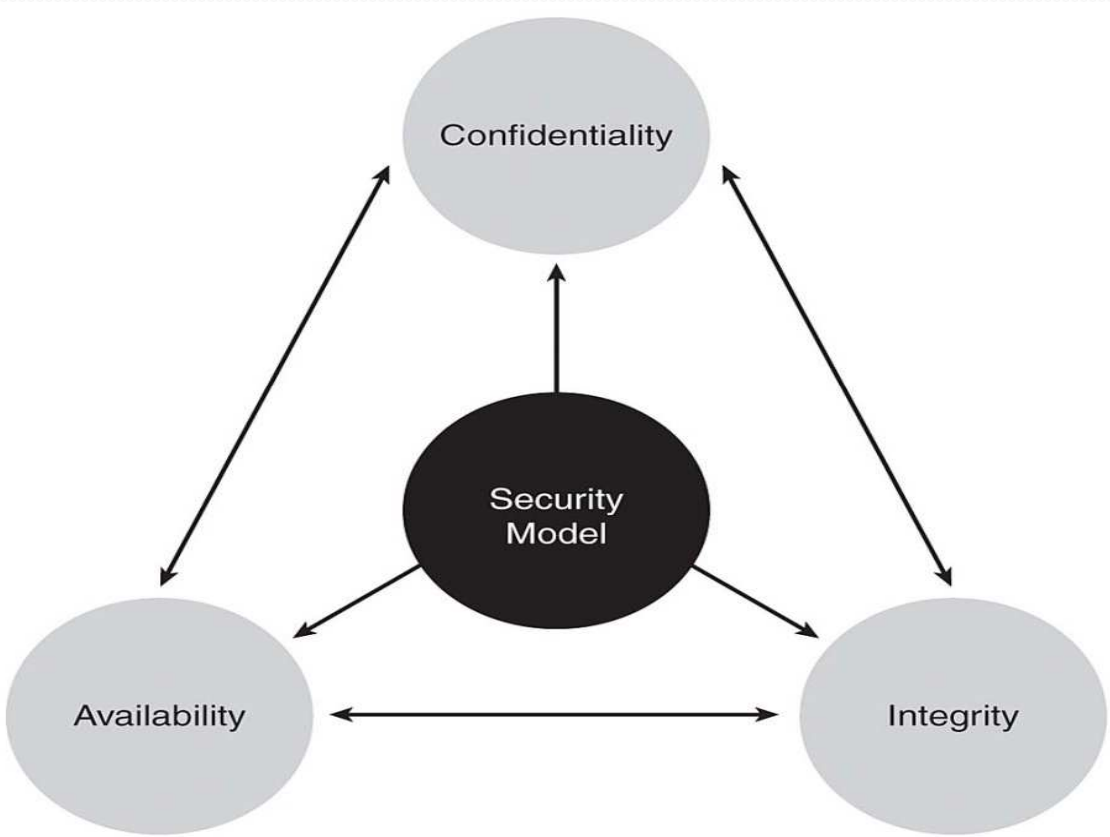
- Ping of death


CYBER
CRIMINAL

WHO IS DOING ALL THIS

- University Students for leisure and learning case of government exploit;
- Organized hacktivists
- Disgruntled employees
- Professional hackers
- Employees with sizeable experience and stay aaat the firm

COMPUTER SECURITY



HOW

- Continually evaluate IT Risks;
- Keep it Simple and prioritize resources based on sensitivity;
- Maintain and Review Logs
- Play victim and monitor access to critical information
- Do not lock out the attacker- use of honey pots and other mechanisms of detecting fraud as it occurs

COMPUTER SECURITY - TOOLS

- Proactive ICT Assessments
- Intrusions Detection Systems
- Proper Firewall Configuration
- Encryption of Data
- Use HTTPS for internet banking

CYBER LAWS

- Law governing cyber space; encompasses laws relating to:
  — Cyber Crimes and origin of IP

  — Intellectual Property

  — Data Protection and Privacy

- Intellectual property: it refers to legal concept which refers to creations of the mind for which exclusive rights are recognized.

- Data protection and privacy: it refers to effective legislation helps minimize monitoring by governments , regulate surveillance by information is properly protected.

HANDLING CYBER CRIME INCIDENCE

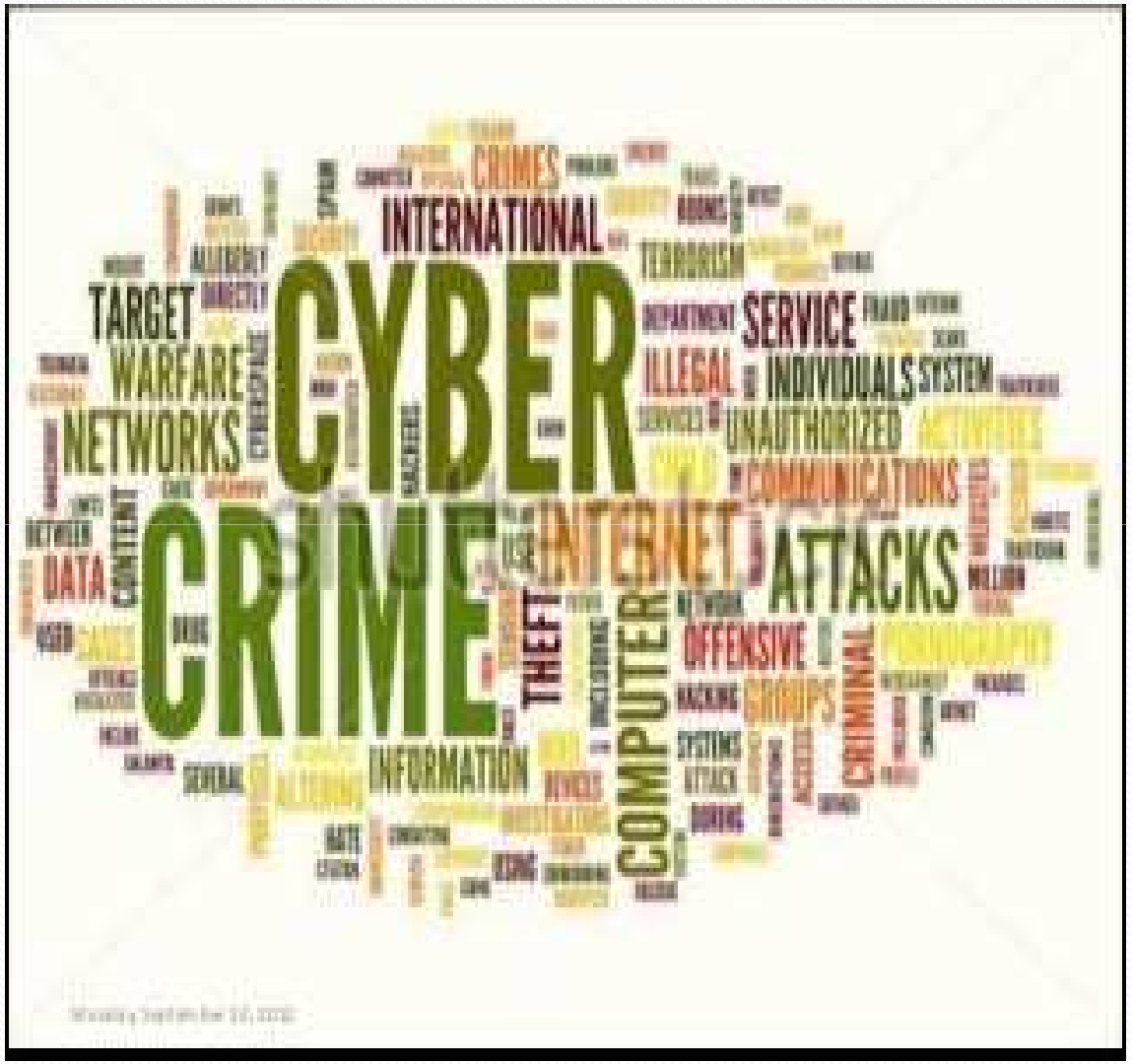
- Disable and log off a specific user account to prevent access;
- Preserve activity and event logs as much as possible;
- Disable and log off a group of user accounts which access a particular service that is being attacked;
- Disable and dismount specific (network) devices, for instance disk devices that are being swamped.

- Disable specific applications, for example, an e-mail system subjected to a SPAM attack.

- Close down an entire system, and divert processing to an alternative or backup service on a secondary network.

CONCLUSION

- As such, investigators will know what and which materials to search and seize, the electronic evidence to recover, and the chain of custody to maintain.


CYBER
CRIME
INTERNATIONAL
CRIMES
TARGET
WARFARE
NETWORKS
SERVICE
INDIVIDUALS
ILLEGAL
UNAUTHORIZED
COMMUNICATIONS
INTERNET
ATTACKS
DATA
THEFT
COMPUTER
OFFENSIVE
GROUPS
CRIMINAL
INFORMATION
TERRORISM
SYSTEM

QUESTION AND ANSWER