Cyber Security:- an overview

AfNOG 2011, Dar Es Salaam

Computer Emergency Response Team Track

By

Marcus K. G. Adomey

OVERVIEW

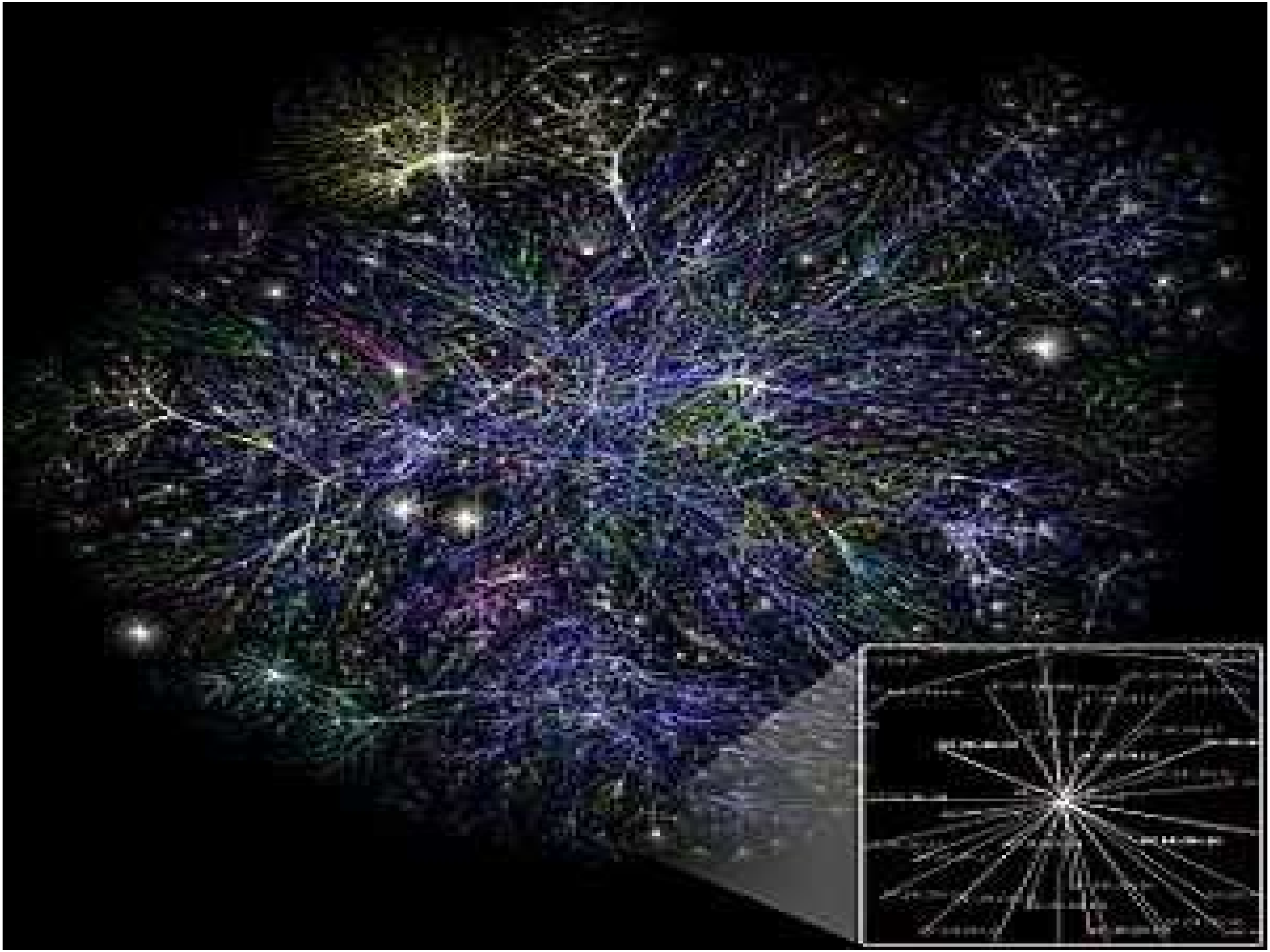
- ✓Internet
- ✓What is the Internet
- ✓The use of the Internet
- ✓Problems related to the Use of the Internet: Security
- ✓What is Security?
- ✓Categories of Security Incidents
  - ▪Hacking
  - ▪Malware
    - o Virus, Worms, BotNet, Spyware, Adware, Trojan Horse
  - ▪DDOS Attack
  - ▪Other types of Security Incidents
- ✓Important Landmark: CERT

Internet

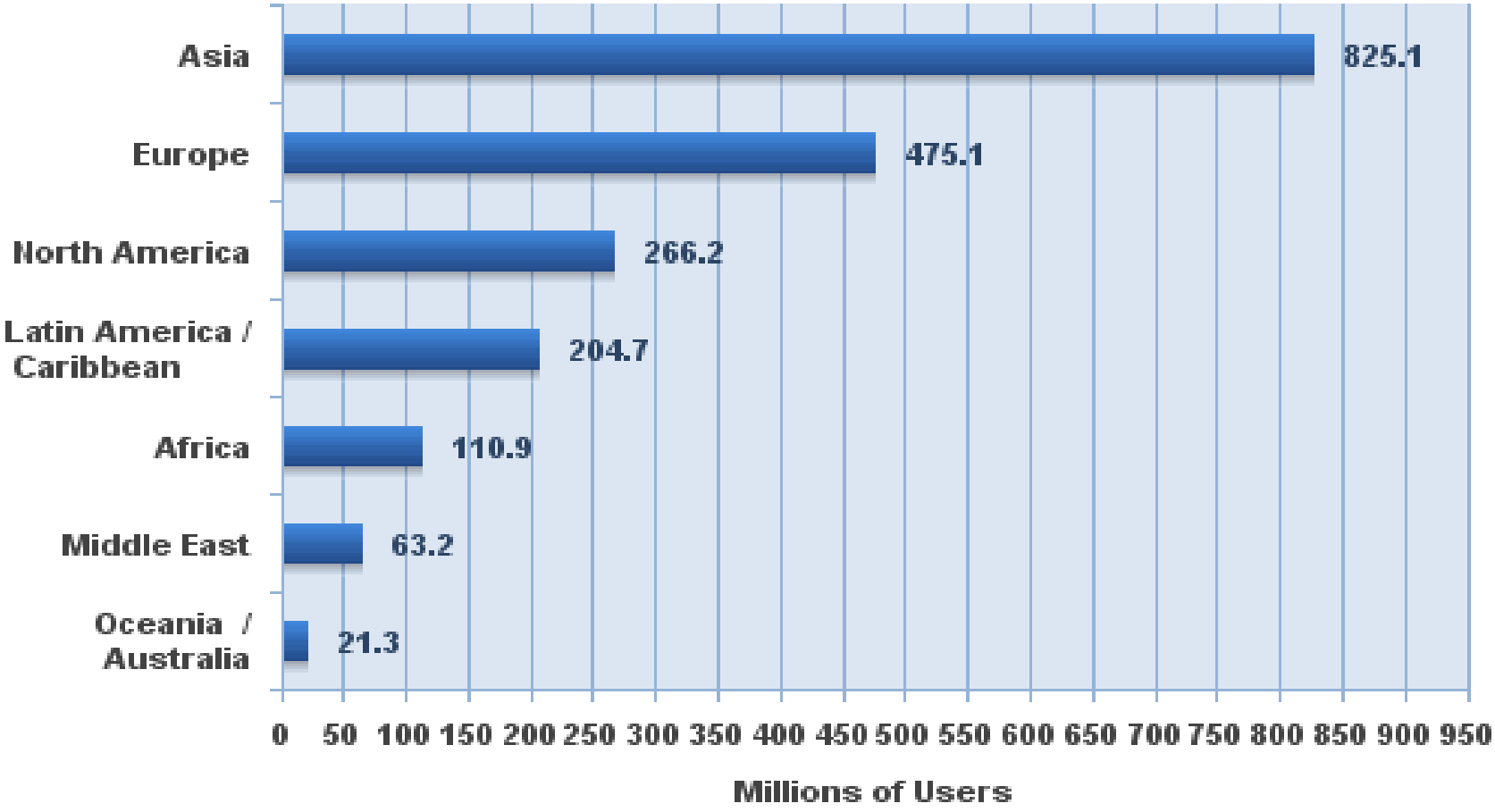
INTERNET:- Definition

- ✓ *The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide.*
- ✓ *It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies.*

Source: Wikipedia

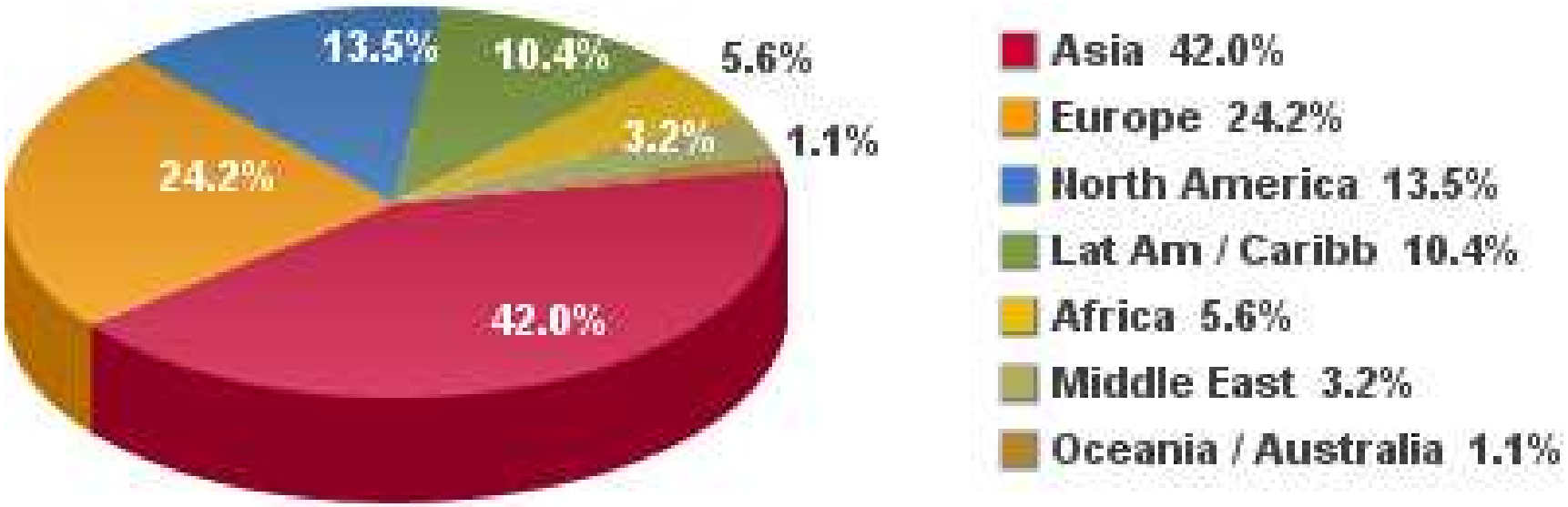


Internet Users in the World by Geographic Regions - 2010



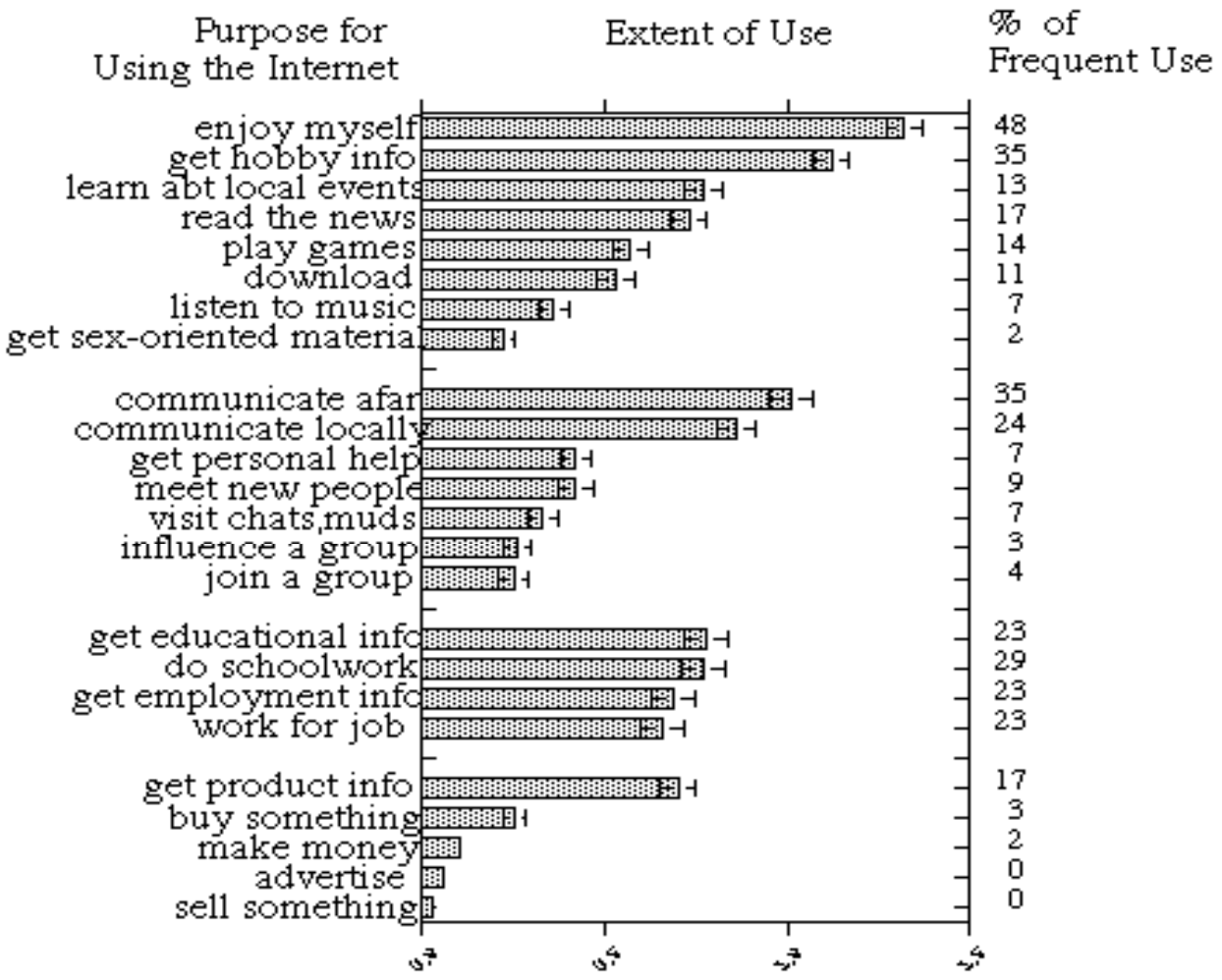
Source: Internet World Stats - www.internetworldstats.com/stats.htm
Estimated Internet users are 1,966,514,816 on June 31, 2010

Internet Users in the World
Distribution by World Regions - 2010



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 1,966,514,816 Internet users on June 30, 2010

WHY PEOPLE USE THE INTERNET



N=212

Bar length is mean extent of use,
where 0=never, 1=occasionally, 2=frequently

Numbers = % who report doing activity frequently

Robert Kraut, Vicki Lundmark, Sara Kiesler, Tridas Mukhopadhyay, William Scherlis
Carnegie Mellon University

PROBLEMS RELATED TO THE USE OF THE INTERNET

SECURITY

BRAINSTORMING

What is Security (Definition)?

SECURITY - Definition

There is no clear cut definition

Security is a process, not an end state.

***Security is the process of maintaining an acceptable level of perceived risk*.**

No organization can be considered **"secure"** for any time beyond the last verification of adherence to its security policy.

- ***If your manager asks, "Are we secure?"***
- ***you should answer, "Let me check."***
- ***If he or she asks, "Will we be secure tomorrow?***
- ***" you should answer, "I don't know."***

Such honesty will not be popular, but this mind-set will produce greater success for the organization in the long run.

SECURITY - Features

A key aspect of Information Security is to preserve the confidentiality, integrity and availability **(CIA)** of an organization's information.

- ✓ **Confidentiality.** Assurance that information is shared only among authorized persons or organizations.
- ✓ **Integrity.** Assurance that the information is authentic and complete.
- ✓ **Availability**. Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

COMPUTER SECURITY INCIDENT

Each organization will need to define what a computer security incident is for their site. Examples of general definitions for a computer security incident might be:

Any real or suspected adverse event in relation to the security of computer systems or computer networks

-or-

Any computer security related event caused by humans, including both intentional and accidental ones.

-or-

The act of violating an explicit or implied security policy

Security Incident Categories

- Hacking:- Internal and External
- Malware
- Denial of Service
- Compromised Asset
- Unlawful Activity
- E-mail
- Policy Violations

HACKING

Hacking

There is an on-going debate about the definition of the word hacker.

- ✓ A hacker can be anyone with a deep interest in computer-based technology; it does not necessarily define someone who wants to do harm.
- ✓ The term attacker can be used to describe a malicious hacker. Another term for an attacker is a black hat.
- ✓ Security analysts are often called white hats, and white-hat analysis is the use of hacking for defensive purposes.

Methods of attack

Password cracking doesn't always involve sophisticated tools.

- ✓ It can be as simple as finding a sticky note with the password written on it stuck right to the monitor or hidden under a keyboard.
- ✓ Another crude technique is known as "dumpster diving," which basically involves an attacker going through your garbage to find discarded documentation that may contain passwords.

Greater Levels of Sophistication of Attacks

Dictionary attack

A simple dictionary attack is by far the fastest way to break into a machine. A dictionary file (a text file full of dictionary words) is loaded into a cracking application (such as L0phtCrack), which is run against user accounts located by the application. Because the majority of passwords are often simplistic, running a dictionary attack is often sufficient to the job.

Hybrid attack

Another well-known form of attack is the hybrid attack. A hybrid attack will add numbers or symbols to the filename to successfully crack a password. Many people change their passwords by simply adding a number to the end of their current password. The pattern usually takes this form: first month password is "cat"; second month password is "cat1"; third month password is "cat2"; and so on.

Brute force attack

A brute force attack is the most comprehensive form of attack, though it may often take a long time to work depending on the complexity of the password. Some brute force attacks can take a week depending on the complexity of the password. L0phtcrack can also be used in a brute force attack.

Internal Hacking

Internal attackers are the most common sources of cracking attacks because attackers have direct access to an organization's systems.

Example of Internal Hacker:

- ✓ A disgruntled employee
- ✓ The help desk technician

External Hacking

External attackers are those who must traverse your "defense in depth" to try and break into your systems. They don't have it as easy as internal attackers.

The first common form of external attack is known as Web site defacing. This attack uses password cracking to penetrate the systems that the attacker wants to deface.

Another possible password cracking attack is when an attacker tries to obtain passwords via Social Engineering.

Social Engineering is the tricking of an unsuspecting administrator into giving the account ID and passwords over to an attacker.

Cases of attacks

- ✓ Kevin Mitnick in 1995 was arrested again for breaking into various computers and downloading 20,000 credit card numbers

- ✓ In 1994, Vladimir Levin accessed the accounts of several large corporate customers of Citibank via their dial-up wire transfer service and transferred funds to accounts set up by accomplices in Finland, Germany and Israel, Netherlands and The United States. In February 1998 he was convicted and sentenced to three years in jail, and ordered to make restitution of US$240,015. Citibank claimed that all but US$400,000 of the stolen US$10.7 million had been recovered.

- ✓ In December 2010, a bank in Ghana has been hacked and the hackers have succeeded in transferring and stealing a huge amount which has led the bank to pay seven million US dollars to Visa International. For corporate image protection the name of the two banks mentioned will not be disclosed.

- ✓ Recently, on the March 12, 2011, Australian Police confirmed the statement of Commonwealth Bank that about 40 Automatic teller machines (ATMs) of Commonwealth Bank in Australia spat out tens of thousands of free dollars in Sydney after a computer glitch turned into a nightmare for the bank.


ATM
© 2010 CBS Interactive


AUTOBANK
Love
is free!

- ✓ In 1995, Richard Pryce, age 16, and Mathew Bevan, age 21, (All British) broke into the Rome Air Development Center, Griffiss Air Force Base, NY, and before authorities became aware of their presence (five days later) they had penetrated seven systems, copied files including sensitive battlefield simulations, and installed devices to read passwords of everyone entering the systems.

MALWARE

Malware, short for MALicious softWARE, is software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Example of Malware:- Stuxnet

Among the dangerous Malware one can name the recent and famous Stuxnet discovered during the last quarter of the year 2010. Stuxnet is viewed by top IT security expert as potentially the most dangerous piece of computer malware discovered last year. It has been developed on an unprecedented scale and has the ability to target and control specified industrial machinery. Stuxnet is a 100-percent-directed cyber attack aimed at destroying an industrial process in the physical world. Others are speculating that it may be used to target a nuclear plant in Iran.

MOVIE:- Stuxnet

What is virus?

A computer virus is a computer program that can copy itself and infect a computer.

What is a BOTNET?

- ✓ The term BotNet is short for ro**BOT NET**work. Criminals distribute malware that can turn computer into a bot (roBOT) also known as a zombie. When this occurs, the infected computer can perform automated tasks over the Internet, without the owners being aware of them.
- ✓ Criminals typically use bots to infect large numbers of computers. These computers form a network, or a botnet.
- ✓ Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. If a computer becomes part of a botnet, it might slow down

What is a worm?

A computer worm is a self-replicating Malware computer program. It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. This is due to security shortcomings on the target computer.

MOVIE:-
Virus, Botnet and Worm

Adware

A software program that is designed to run once a web page has been accessed. This is usually in the form of banner or popup advertisements. Adware can also be designed to be installed on your system without your consent or knowledge.

What is a Trojan horse?

A trojan horse, or trojan, as the name implies, secretly carries often-damaging software in the guise of an innocuous program, often as an email attachment.

The file name itself is normally misleading to entice you to open it.

Spyware

A program designed to steal confidential information (eg credit card details, user names, passwords etc.). Software downloaded from the Internet may contain spyware and other forms of malware.

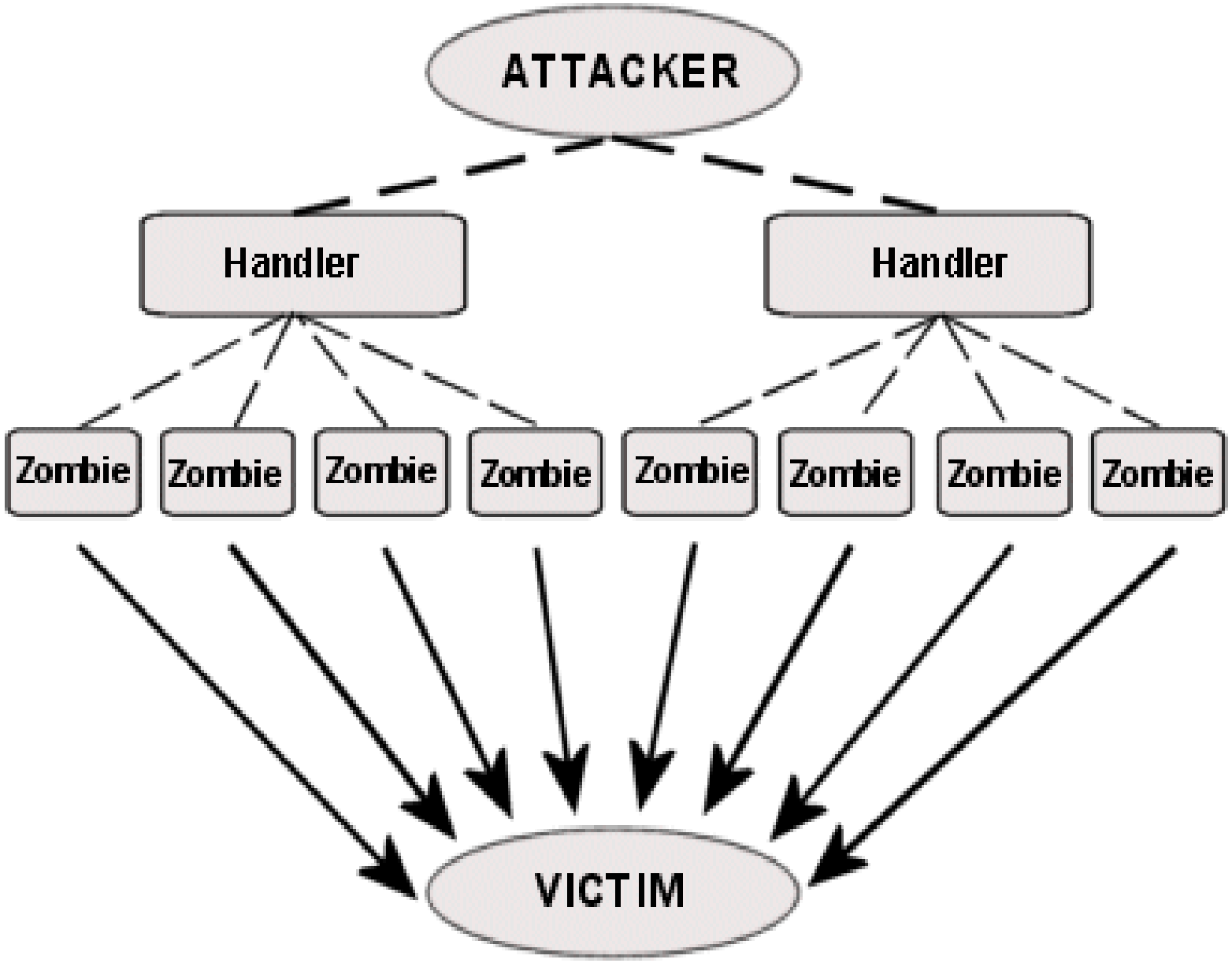
MOVIE:- SPYWARE

Denial of Service
DOS or DDOS

- ✓ Denial of service: - In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

- ✓ In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

Architecture of a DDoS Attack



Example of DDOS Attack: Estonia Case in 2007

- ✓ In 2007 an attack on Estonia government is considered by some experts to be the first ever case of cyber war. Estonia is considered the most wired nation in Europe with over 90% of citizens using online banking and even elections being held online. The attack, which has forced many websites to shut down and inflicted losses on the nation's economy, is being described as the first "war in cyberspace"
- ✓ The hackers from used a simple tactic: sending huge amounts of information to the targeted websites simultaneously, causing them to overload and freeze in what is known as "distributed denial-of-service disruptions."

- ✓ *"You couldn't get information; you couldn't do your job. You couldn't reach the bank; you couldn't check the bus schedule anymore. It was just confusing and frightening, but we didn't realize it was a war because nobody had seen anything like that before".*
- ✓ *"I felt the country was under attack by an invisible enemy. It was extremely frightening and uncontrollable because we are used to having Internet all the time and then suddenly it wasn't around anymore,"*

Tuuli Aug, an editor of international affairs at the Estonian daily newspaper "Eesti Paevaleht,"

Estonia's extreme reliance on internet technologies made it especially vulnerable to these attacks.

Compromised Information

Attempt or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property

Compromised Asset

Compromised host (root account. Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.

Unlawful activity

Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.

E-mail

Spoofed email, SPAM, and other e-mail security-related events.

Policy Violation

- Sharing offensive material, sharing/possession of copyright material.
- Deliberate violation of Information security policy.
- Inappropriate use of corporate asset as computer, network, or application.
- Unauthorized escalation of privileges or deliberate attempt to subvert access controls.

REMARK

CYBERCRIME

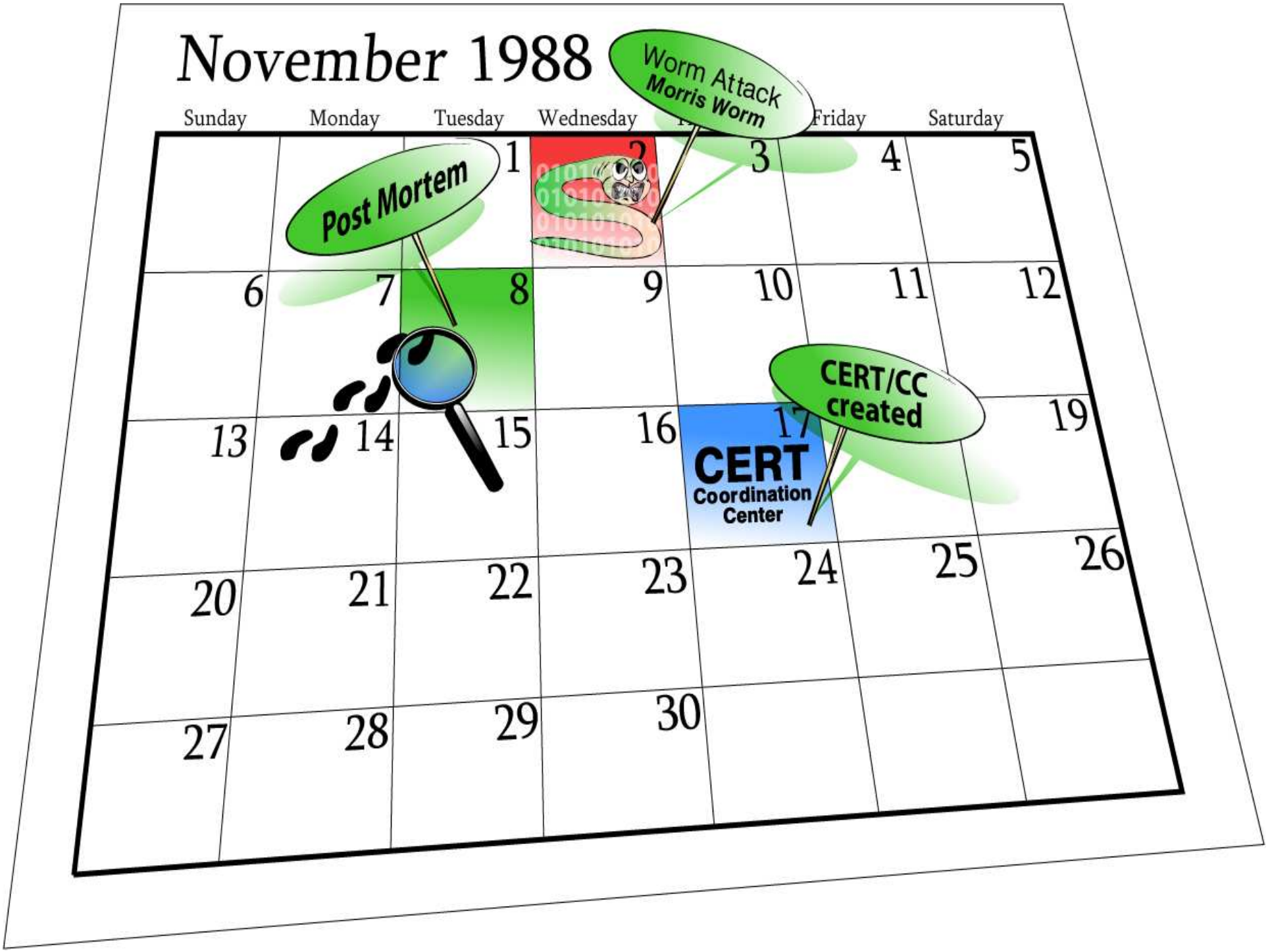
Cybercrime refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.


shutterstock


Matt Murphy


The threat is real

IMPORTANT LANDMARK


November 1988
Worm Attack
Morris Worm
Post Mortem
CERT/CC
created
CERT
Coordination
Center
Sunday
Monday
Tuesday
Wednesday
Friday
Saturday
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
19
20
21
22
23
24
25
26
27
28
29
30

- ✓ **ICT is a single point of failure to business.**
- ✓ **Security is Achilles heels of ICT**

SO

- ✓ **Let us come together under CERT and fight the enemy**

Computer Emergency Response Team - CERT

What is CSIRT

It is an organization or team that provides, to a defined constituency, services and support for both preventing and responding to computer security incidents

Terminology

There exist various abbreviations for the same sort of teams

- **CERT or CERT/CC - Computer Emergency Response Team / Coordination Centre**
- **CSIRT - Computer Security Incidence Response Team**
- **IRT - Incident Response Team**
- **CIRT - Computer Incidence Response Team**
- **SERT - Security Emergency Response Team**

CERT around the world

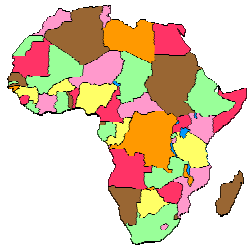
FIRST Teams around the world

IMPACT - International Multilateral Partnership Against Cyber Threats

CERT-Africa

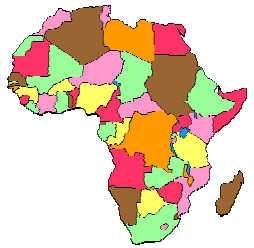
In Africa, few countries have started their security project and fulfilled some good steps; other countries have now started implementing national mechanisms for combating cybercrime and other related threats; however, a sizeable number of African countries still do not have a strategic plan and are unable to start their first actions.

CERT- AFRICA : The African response to capacity development on cyber security in Rwanda Kigali, 30th of Mai 2010,



CERT-Africa: OBJECTIVES

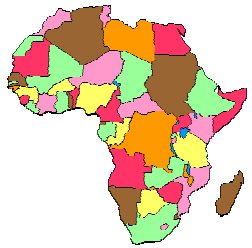
CERT-AFRICA initiative is being proposed as a means for providing a continental platform for African countries to enhance regional and international cooperation on information security; through the platform, countries will assist each other to establish national Computer Security Incident Response Teams (CSIRT) and thereby improve their incident handling capabilities; also, the platform will provide technical support and look for financial resources.



Promoters

- Nii Narku Quaynor (Ghana)
- Pierre Dandzinou (Benin)
- Haythem EL MIR (Tunisia)
- Perpétus Jacques Houngbo (Benin)
- Jean Robert Houtomey (Togo)
- Vincent Ngundi (Kenya)
- Mohamed Ibrahim (Somalia)
- Marcus K. G. Adomey (Ghana)

IN PARTNERSHIP WITH APCERT AND JPCERT



National CERT

National CSIRTs can play an important role by helping their internet-connected sites protect their systems, detect, recognize, and analyze compromises to the security of those systems, protect themselves from malicious activities, and when cybersecurity incidents occur, quickly and effectively coordinate and respond to attacks.

These teams can also be evangelists in promoting and helping other organizations within their national borders build effective incident management capabilities.

National CERT: Benefits

From a technical security standpoint national teams can

- ✓ serve as a trusted point of contact
- ✓ develop an infrastructure for coordinating response to computer security incidents within a country.
- ✓ develop a capability to support incident reporting across a broad spectrum of sectors within a nation’s borders
- ✓ conduct incident, vulnerability, and artifact analysis.
- ✓ disseminate information about reported vulnerabilities and corresponding response strategies
- ✓ share knowledge and relevant mitigation strategies with appropriate constituents, partners, stakeholders and other trusted collaborators.

- ✓ participate in cyber “watch” functions;
- ✓ encourage and promote a community of national and regional teams that share data, research, response strategies,
- ✓ help organizations and institutions within the nation develop their own incident management capabilities.
- ✓ make general security best practices and guidance available through publications, web sites, and other methods of communication.
- ✓ promote or undertake the development of education, awareness and training materials appropriate for a variety of different audiences.
- ✓ identify and maintain a list of CSIRT capabilities and points of contact within a country.

Local CERT

Under National CERT there could be some of the following CERT:

- GovCERT
  - MilCERT
  - PoliceCERT
  - FinanceCERT
  - HealthCERT
- Academic CERT
- ISPCERT
- BankCERT
- IndustryCERT

Thank You!!!