COMESA

Deterring CyberCrime

August 25th – 28th, 2008
Lusaka, Zambia

Presenter: Isabel Nshimbi
Information Systems Analyst
COMESA Secretariat

“Security is not a product, but a process..”

Focus:

- Definitions
- Secretariat Approach
- Levels of Security
- Regional Initiatives
- Best Practises

CyberSecurity and CyberCrime…

CyberSecurity:

- The protection of data and systems in networks that are connected to the Internet (PCMag)

CyberCrime:

- Crimes perpetrated over the Internet, typically having to do with online fraud

Multi-billion dollar problem

The Crimes…

- downloading illegal music files
- stealing money from online bank accounts
- creating and distributing viruses
- posting confidential business information on the Internet
- identity theft
  - phishing
  - pharming

Broad scope of criminal activity, so we have to be careful where we enter our personal information

The Criminals…

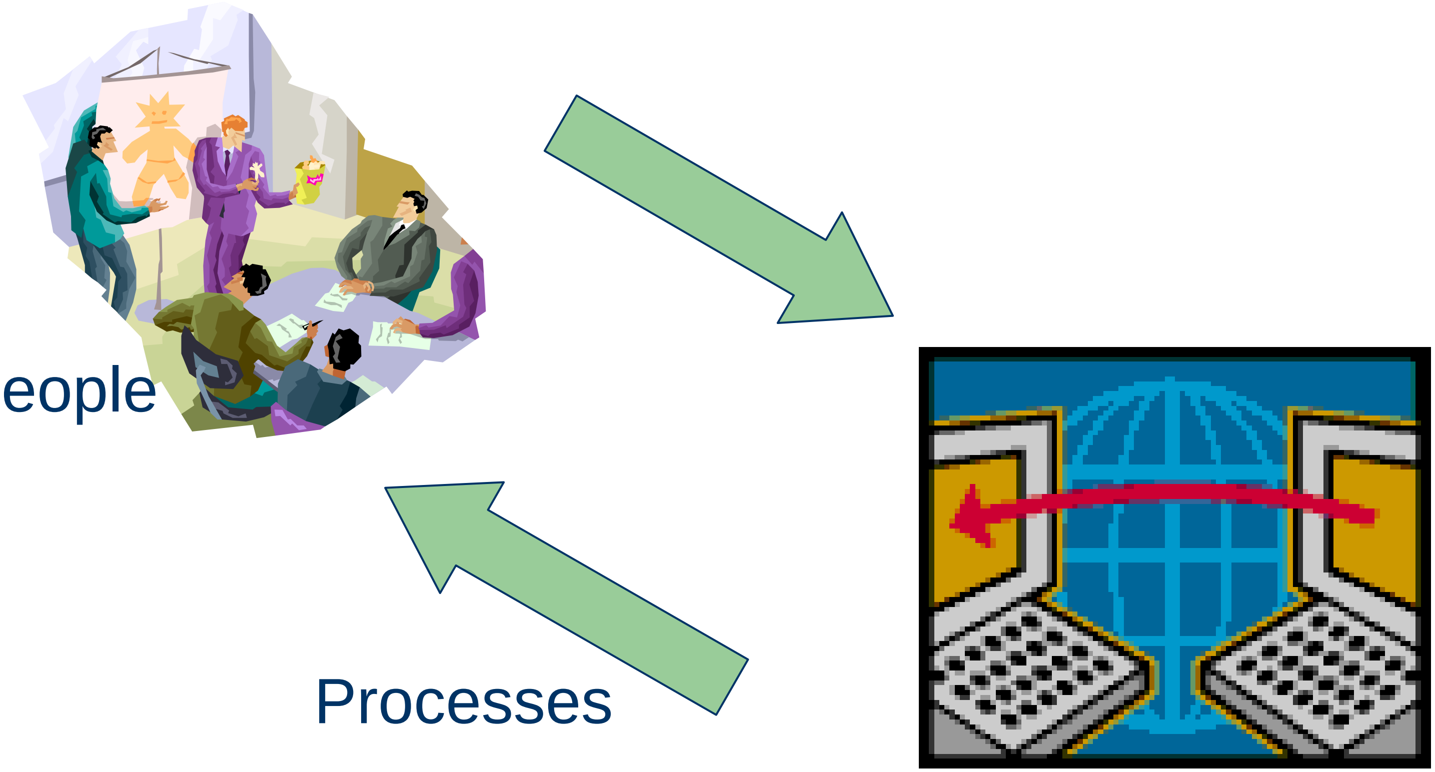
- Hackers, alone or in groups
  - Deceptive Duo
  - Global Hell
  - Darkside Hackers
  - Conflict
- Virus Creators
- Employees (former, disgruntled…)
- Financial Institution Insiders

Cases…

- 1999
  - Hacking into and De-Facing of Government Website in Zambia
  - Hackers gained access to personal e-mail accounts on free Hotmail service
- 2005
  - Intrusions into Government Computers and Defacing Websites in US by the Deceptive Duo
- 2008
  - Former Employee in local firm in Phillipines – access to and copying of firm’s secret information

COMESA’s Strategy

What is Involved?

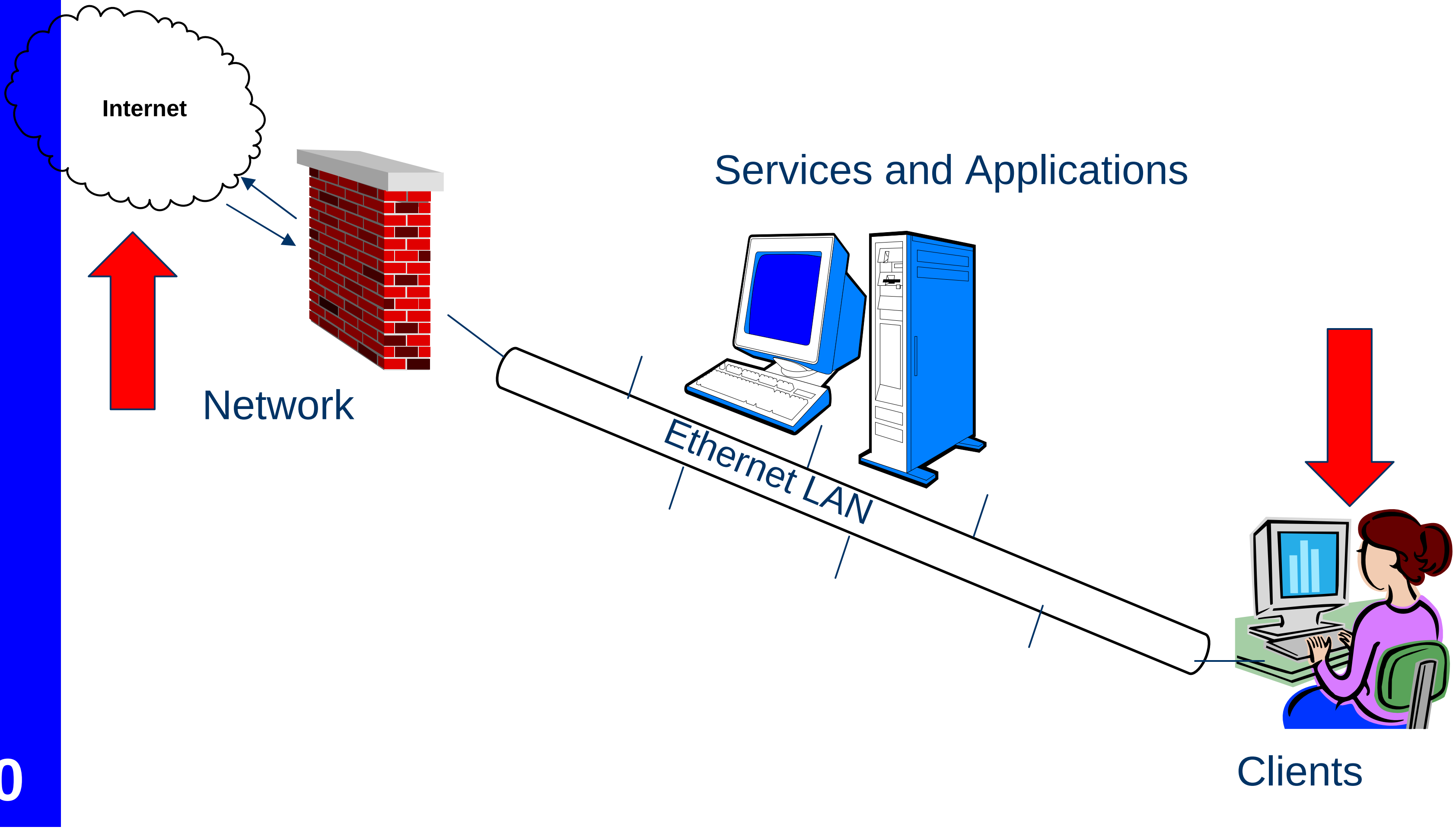


People

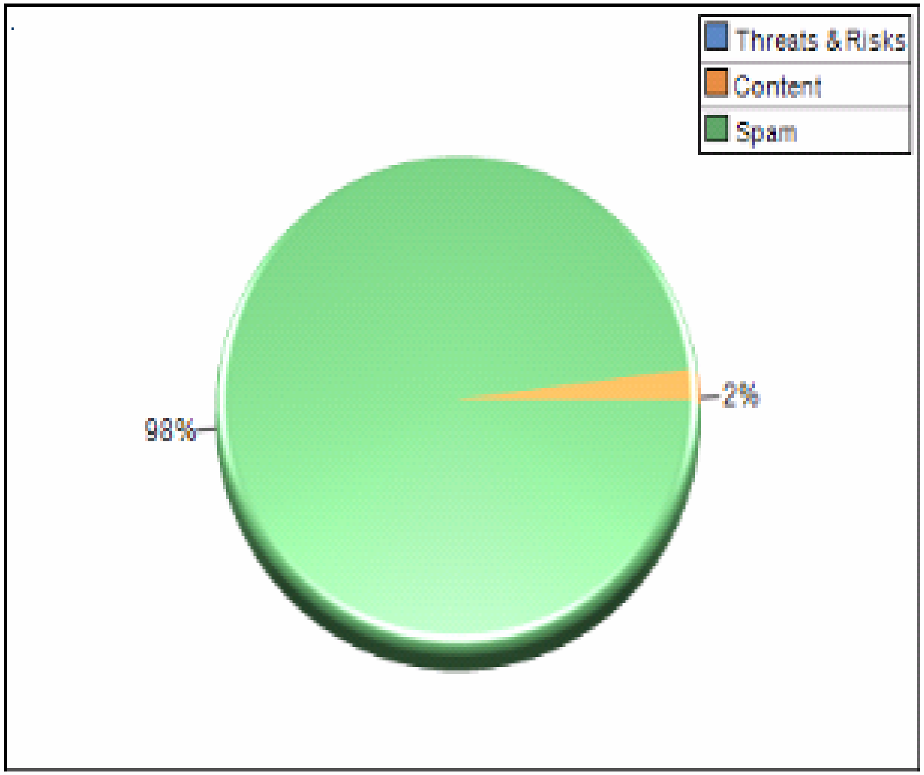
Processes

Technology

Deterrents… At Three Levels



Detected Threats / Attempts

- 

Regional Initiatives

- **e-Legislation Programme**
  - Study on e-Legislation
  - Workshop in September, 2007
  - Second workshop in October, 2008

e-Legislation Study

Legal Certainty

Legal Security

Legal
Protection

Legal Deterrents

Legal Deterrents

- •Law Reform Initiatives
  - •Substantive Criminal Law
  - •Procedural Criminal Law
- •International Cooperation
- •Regional/ International CyberForensics Organ?

Best Practises

- Do not send sensitive data in unencrypted form
- Acquire security expertise
- Do not reinvent the wheel
- Safe Disposal of Old computers
- Clear Policies and Procedures
- Review, review, review security regularly

Thank You