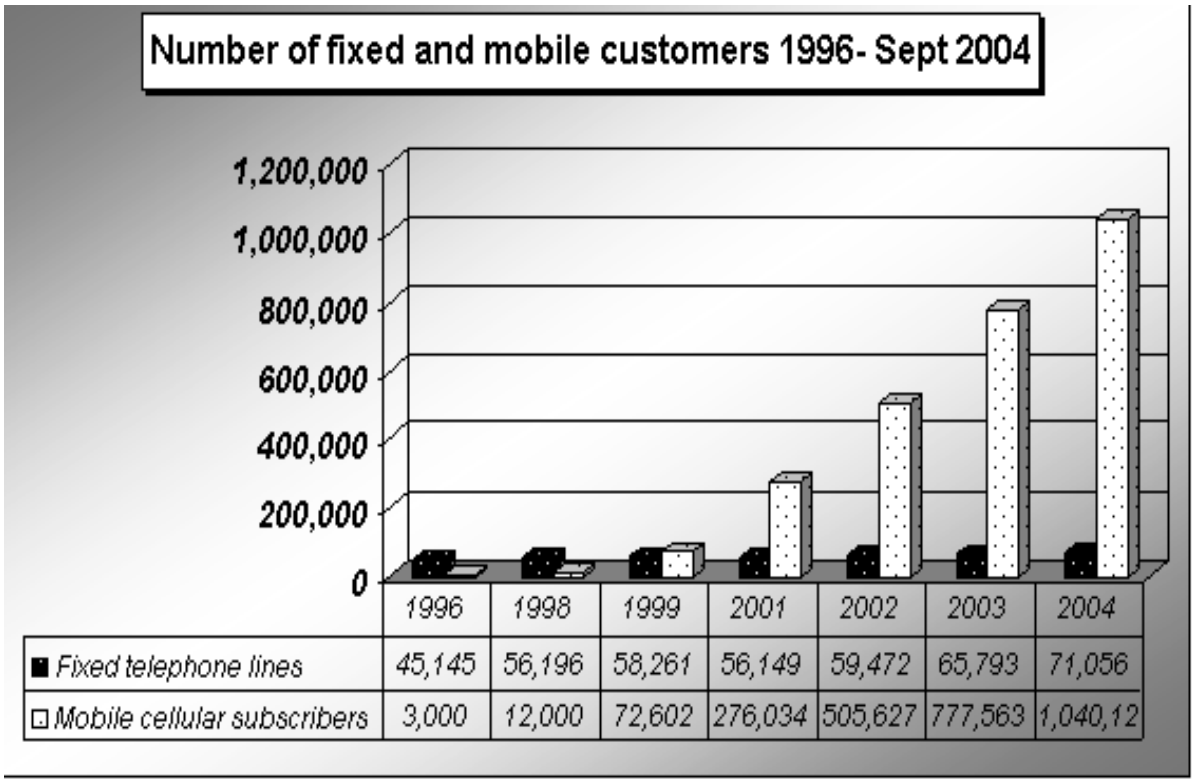
ITU WSIS THEMATIC MEETING ON CYBERSECURITY, GENEVA, SWITZERLAND, 28 JUNE -1 JULY 2005.

PAPER ON THE STATE OF CYBERSECURITY IN UGANDA.

BY : UGANDA COMMUNICATIONS COMMISSION

1.0: Background

Uganda, like many countries, has embraced ICT use in its entire social, economic and political structures. Uganda with a population of about 26 millions people, has an average real rate of GDP growth has been 6.9 per annum since 1990. The current teledensity of 4.2%, combining both mobile and fixed , is still low , but steadily growing internet utilization. This can be seen in the figure below.



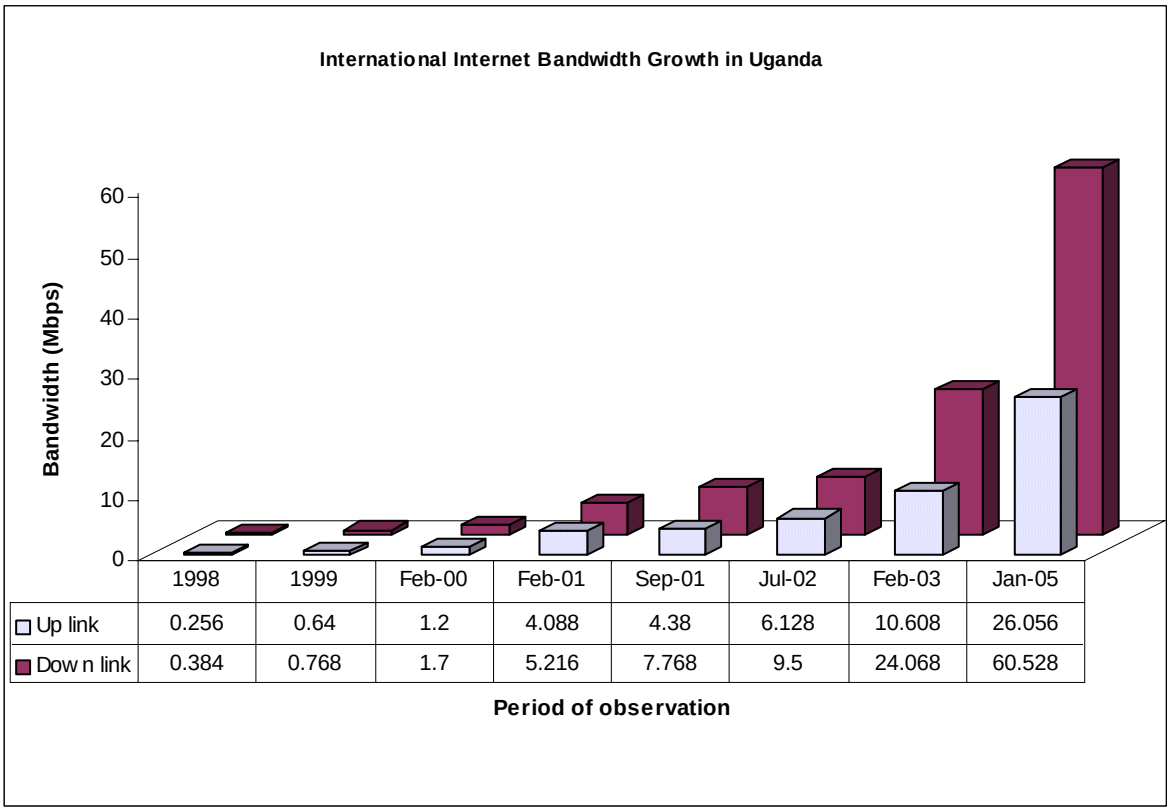
	1996	1998	1999	2001	2002	2003	2004
Fixed telephone lines	45,145	56,196	58,261	56,149	59,472	65,793	71,056
Mobile cellular subscribers	3,000	12,000	72,602	276,034	505,627	777,563	1,040,12

The above facts to one important fact that ICTs in Uganda are increasing in importance and uptake is also increasing, therefore issues of ICT security are important.

This increased use of computers among organizations has seen many finally connect up to the Internet even if for only email services. The growth in bandwidth as shown in figure 2, and the growth in the number of domain names registered under the .ug Top Level Domain in figure 3 give a fair representation of this increased use of the Internet. Many companies have

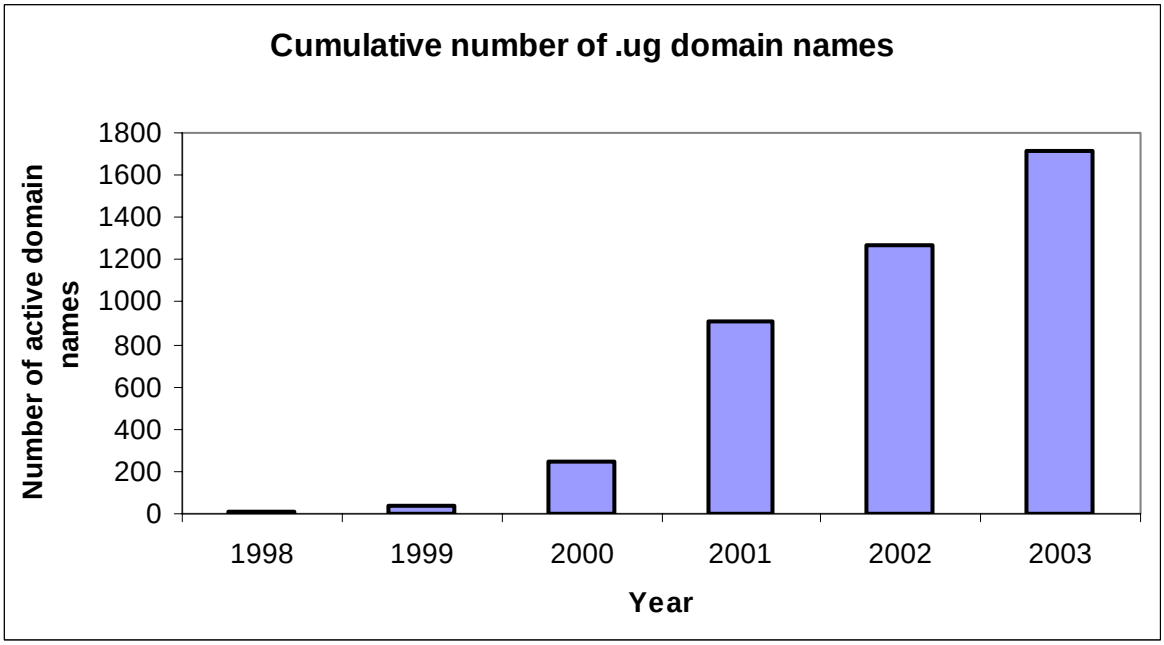
opted to register using generic top level domain names like .com and .net and are therefore not included in the numbers shown in figure 3.

Figure 2: Growth of bandwidth



	1998	1999	Feb-00	Feb-01	Sep-01	Jul-02	Feb-03	Jan-05
Up link	0.256	0.64	1.2	4.088	4.38	6.128	10.608	26.056
Dow n link	0.384	0.768	1.7	5.216	7.768	9.5	24.068	60.528

Figure 3: Growth of number of Domain names.



This trend among organizations has provided a number of people the opportunity to obtain access to the Internet which at their work places and slowly discover the vast potential of the Internet as an information resource.

Unfortunately the growth of the knowledge of the potential internet has not developed with the awareness of the potential dangers of related to cyber attacks. Many Ugandans remain unaware of cyber attacks.

Uganda has already adopted a National ICT framework, whose major aim is it to ensure that ICTs play their rightful role in the development of the country. This coupled with Uganda's new policy, which is due for adoption by cabinet, has put in place several objectives which are specifically geared towards increasing both penetration and utilization of both traditional voice services and data and internet services.

With this anticipated growth in ICTs, security of both the infrastructure and databases is vital.

2. Status of Cyber Security in Uganda.

Up until now, the owners of the available communications networks and databases, are solely responsible for their, both cyber and physical security. There has not been a centralized system to ensure an overall country security.

Big organizations owning communications and data networks have their own individual policies covering a range of security related issues.

Individuals who have internet access are heavily reliant on the Internet Service Providers to provide them with some level of security. More sophisticated users have additional security through use of anti viruses, passwords and firewalls.

Majority of internet users access internet through organization networks, and are hence are as protected as the organization are protected. Otherwise majority of the public access internet through public cafes in which case they are as protected as the Internet Service Providers serving them and as the cafes are protected.

In the recent past Uganda as a country has not experienced large scale service interruptions or loss of data, due to cyber attacks. Most of the related attacks have been on data bases and computer networks and have been experienced by organizations and individuals, but not at a country level.

There have been few reported cases of attacks on communications networks, although virus attacks are increasingly being reports on mobile phones.

In the recent past, most of the problems have been “Indirect” attacks, not aimed at any particular organization or individual, through viruses which have been transferred from one computer to another through sharing of diskettes. This is somewhat lessening as users have become aware of the dangers of sharing diskettes, and the increasing use of memory sticks rather than diskettes. The other possible reason for reduction in this kind of spread is the increasing networking of computers which means sharing files is done via the intra-network.

The emerging cyber problems are through downloading of files from corrupted sources. This is exponentially increasing as more and more people are downloading a lot of information from the internet.

“Direct” attacks, (aimed at organization or individuals), of networks and databases have not yet been rampant. There have been few software break-in reported, mainly in the banking sector.

3. Existing methods of protections

Organizations which feel vulnerable have formulated organization ICT policies, which among things address security concerns. Such organizations make use of firewalls, virus guards etc to protect their networks and databases.

Such organizations include;

- Academic institutions
- Banks
- Non-governmental Organization
- High Commissions and Embassies.
- Public organizations
- Internet Service Providers
- Telecommunication Service Providers

There is however a limited number of organizations protecting themselves to this level, this is mainly because of the costs involved. Most of the software protection available involves regular renewal of licenses and subscriptions, and these costs are considered by many.

The second reason is that most organizations do not have first hand experience of cyber problems and have little idea of the implications. Most of those who are taking great care have been hit and they know the implications.

The third reason is the lack of awareness of the seriousness of the problems related to cyber attacks.

Individual users stay at the level of using virus guards, and in most cases once the subscription is over, it is not renewed, they just move to another free trail virus guard. This is mainly because of cost implications of keeping up subscriptions to virus protection vendors.

4. The need.

Indeed use of internet, databases and networking of computers is growing. Already;

- Banks have set up operations which really need a lot of security.
- Organizations are now installing information systems which are interactive with external users
- Academic institutions are putting a lot of their services and products on the network, to be accessed externally
- Almost all government entities are going e-government.

There is therefore a need for concerted efforts in addressing cyber security, from within and without. This will not replace the need for each individual person or organization to implement their own personal security, but will look at the broader issues which concern a network of networks in the country.

5. The challenges.

There are several challenges facing the development of a concerted national cyber security program. These include;

i) Lack of awareness

Many individuals and organizations simply have no awareness of the problems of cyber attacks. Such individuals or organizations have ended up not putting in enough efforts in protecting themselves

or protecting others. They have no policy or guidelines in place and they pay little or no attention to such issues.

This category of users forms a very big entry point of problems of viruses and their networks being used by other networks to launch malicious attacks.

ii) Cost of Protection

The cost of protection is still considered "high" mainly because it is really high in terms of the regular costs of buying or subscribing to protection agents. The cost is still high because some do not know the costs involved in case of an attack.

Many simply give up and other resort to substandard products, when they feel that the cost of protection is high for them..

iii) Lack of Coordination

As the networks and databases increase both in size and importance, there is going to be need for coordination for;

- Sharing information and experience
- Early warning
- Back up and recovery support.

Many countries have such coordination bodies, which usually comprise of government and private sector working together.

iv) Human Resource

The amount of skilled labor in both computer networking and various Internet applications is increasing although it is not yet reached the necessary levels to address issues related to cyber attacks. More relevant training is needed to address this inadequacy.

v) Lack of necessary laws

Experience elsewhere has shown that the starting point of protection through enacting appropriate laws which declare what is legal and illegal through laws.

In Uganda many of the laws in place today were drawn up before ICTs, more specifically the Internet, became significantly popular and as such did not properly address the problems being

encountered today, such as cyber attacks. Fortunately the Uganda Law Reform Commission, in collaboration with other stakeholders, is rigorously addressing these issues.

Some of the bills in the offing, which are contributing towards addressing the challenge of cyber attacks include;

- E-transactions Bill,
- The Computer Misuse Bill,
- Electronic Signature Bill.
- Information Bill

These cover computer misuse, facilitation of electronic transactions, consumer protection, and limitation of service providers' liability, privacy protection, intellectual property rights and security.

6. Current Efforts.

The main activity towards cyber security issues is the formulation of the relevant laws , which will result in the setting up of the necessary authorities to address such issues.

Unfortunately cyber threats will not wait for one to be prepared to strike, so it is important to start moving, within the existing legal boundaries.

The Uganda Communications Commission, as a big stakeholder, with security concern of public communication networks, is taking some steps in addressing the challenges of cyber security. UCC:

- Requires, through licenses issued, service providers to set up adequate protection of their networks. There is provision to review these regularly, to determine their suitability. Cyber threats are considered to be among the threats operators need to protect themselves against.

- Has joined both Kenya and Tanzania, as members of EARPTO, to among other things, raise awareness of the importance of the issues of security at regional levels. This is aimed at setting up a voluntary coordination body to deal with early warning and sharing of information. This, for the moment will only cover telecommunication networks but it is hoped that other bodies can join in.

- Is raising awareness of telecommunication subscribers through its consumer awareness programs about issues of cyber attacks.

7 Conclusions.

Uganda like many developing countries, has embraced ICTs as an important tool of development, though at still relatively slow pace, take up of ICTs is growing. Unfortunately lack of awareness of security issues related with ICTs still remains rampant among most users in Uganda.
If not attended to, cyber security may turn out to be a hindrance to utilizing this important tool of development.

Two key issues can be pointed out here;

- The lack of awareness, which must be addressed as soon as possible, and
- The cost of security, which is going higher with time.

Uganda is of the view that both WSIS and ITU have a role to play in making cyber space secure enough to be trusted.