ETIOPIAN TELECOMMUNICATIONS AGENCY

STATE OF CYBER SECURITY IN ETHIOPIA

By Mr. Balcha Reba
Ethiopian Telecommunications Agency
Standards and Inspection Department
Head, Standards Division
email: tele.agency@ethionet.et

June 2005

Table of Contents

1. INTRODUCTION 2
2. BACKGROUND 2
3. STATUS OF CYBERSPACE SECURITY IN ETHIOPIA 4
4. EXISTING SECURITY TECHNOLOGY 5
5. CONCLUSION 6

1. INTRODUCTION

Information security (InfoSec) is the protection of information and its critical elements, including the systems and hardware which use, store and transmit that information. Information security includes the broad areas of information security management, computer and data security management, computer and data security, and network security. To protect information and its related systems, tools such as policy, awareness, training and education, and technologies are of vital importance. Security is the quality or state of being secure, to be free from danger. In other words, security can be defined as building protection against adversaries. The security of information and its systems entails securing all components and protecting them from potential misuse by unauthorized users.

As global networks expand the interconnection of the world's information systems, the smooth operation of communication and computing solutions becomes vital. However, recurring events such as virus and worm attacks and the success of criminal attackers illustrate the weaknesses in current information technologies and the need to provide heightened security for these systems. To put in another way, as the world becomes more and more dependent on networks of computers, it also becomes increasingly and dangerously vulnerable to cyber intrusion and cyber terrorism. Thus, requiring implementation of information security. Now days, the internet has brought millions of unsecured computer networks into communication with each other. The security of each computer's stored information is contingent on the level of security of every other computer to which it is connected.

2. BACKGROUND

The creation of information security program begins with the creation and/or review of the organization's information security policies, standards and practices. Policies shall be considered as the basis for all information security planning, design, and deployment.

Policies do not specify the proper operation of equipment or software. This information should be placed in the standards, procedures and practices of users' manuals and systems documentation.

A policy is a plan or course of action used by an organization to convey instructions from its senior- most management to those who make decisions, take actions, and perform other duties on behalf of the organization. Polices are organizational laws in that they dictate acceptable and unacceptable behavior within the context of the organization's culture. Like laws, policies must define what is right, and what is wrong, what the penalties are for violating policy, and what the appeal process is. Standards, on the other hand, are more detailed statements of what must be done to comply with policy.

The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. These three functions now depend on an interdependent network of critical information infrastructures that we refer to as "cyberspace" to secure this cyberspace a national policy shall be defined in such a way that to prevent or minimize disruptions to critical information infrastructures and thereby protect the people, the economy, the essential human and government services and the national security. Disruptions that do occur should be infrequent, of minimal duration and manageable and cause the least damage possible.

Consistent to the policy in force, the national strategy to secure cyberspace shall have the following objectives:

- Prevent cyber attacks against critical infrastructures.
- Reduce national vulnerabilities to cyber attack and,
- Minimize the damage and recovery time from cyber attacks that do occur.

Despite the facts mentioned above there is no functional cyberspace security policy in Ethiopia. Currently, the Ethiopian ICT Development Authority is preparing national information security standards. However, information security policy should have been

developed earlier to guide the preparation of standards. Due to lack of national cyberspace security policy and associated standards, ICT development programs have very little focus on security components. Similarly, the national network infrastructure and telecommunications service provider, the Ethiopian Telecommunications Corporation, also performs its duties without clearly defined national strategic procedures and guidelines in place. Instead, the Corporation is relying on security elements proposed by vendors and system installers.

3. STATUS OF CYBERSPACE SECURITY IN ETHIOPIA

In 2001, a national taskforce coordinated by the National Computer and Information Center of the Ethiopian Science and Technology Commission initiated Data Disaster Prevention and Recovery Management (DDPRM) program which mainly sought to address data integrity and physical security. The objective of this project was to formulate a policy, which facilitates enabling environment and paves the way for designing of a secure institutional data center. The over all intention was to protect data stored, processed and transmitted through computer system. In addition to this, the project was also supposed to develop guidelines and procedures that support corporate enterprises to put in place their own organizational data security in house policy.

As compared to data security, information security is a broader system which deals with all critical elements and components of an information system namely: Software, Hardware, Data, People, Procedures and Networks. With regard to this, the Data Disaster Prevention and Recovery Management guideline developed by a taskforce organized by Ethiopian Science and Technology Commission is a good move towards adopting strategies to determine the level of protection required for applications, systems, facilities in ICT development and recover from any disaster without serious business discontinuity and major damages and loss to the system and data. However, escalation of the specific data security issue to more general information security systems was found to be mandatory.

In 2004, not long after the restructuring of IT sectors, the Ethiopian Telecommunications Agency took the initiative to invite the Ethiopian Information and Communication Technology Development Authority (EICTDA) and the Ethiopian Telecommunications Corporation (ETC) to discuss on issues of cyberspace security and encryption policy.

On this initiative, the three institutions agreed on importance of cyberspace security policy and formed a joint technical committee, which follows up the process of formulating information security policy and standards. The institutions have also reached at a common understanding that EICTDA has more broader legal framework and resources to lead the initiative. On the basis of this, EICTDA has employed a consultant to conduct a general assessment on how to go forward to develop a national information security strategy and action plan.

Currently, the Ethiopian ICT Development Authority is working on preparation of information security standards. The final document is expected to be finalized and endorsed by the government for implementation as of September 2005. As part of the capacity building process for the ongoing information security programs, the EICTDA has organized training on Information Security Principles to selected government employees working on ICT and related sectors.

4. EXISTING SECURITY TECHNOLOGY

As mentioned in earlier sections, Ethiopia has not yet formulated information security policy and standards. However, currently the ISP is utilizing firewalls, network Intrusion Prevention Systems (IPS), Dial-up protection and packet filtering mechanisms to protect the internet infrastructure, corporate VPNs and Leased lines. Latest spam guards to get rid of viruses or malicious software (malware) are also in place to protect the system.

The existing ISP security systems are based on technical proposal submitted by network installers and vendors. Therefore, it cannot be referred to as a system developed fulfilling all-rounded national information security policy and standards. In addition to this, when

implementing information security in an organization, there are many human resource issues that must be addressed. The organization should thoroughly examine the options possible for staffing information security function. In this regard, in Ethiopia there is a shortage of information security professionals. Hence, organizations are forced to draw on the current pool of information security practitioners.

5. CONCLUSION

In Ethiopia, currently cyber security policy and standards are inexistent. Information security law, ethics and relevant legislation and regulation concerning the management of information in an organization is not yet developed. With absence of these conditions, it will be impossible to think of reliable cyber security issues. Therefore, formulation of cyber security policy and standards shall be given due attention. Furthermore, to develop more secure computing environments in the future, staffing of information security function has to count on the next generation of professionals to have the correct mix of skills and experience necessary to anticipate and mange the complex information security issues. Accordingly, trainings on information security principles are needed to prepare and create professionals of technology to recognize the threats and vulnerabilities present in existing systems and to learn to design and develop the security systems needed in near future. To this effect, the supports being given by Ministry of Capacity Building (MoCB) on promotion of ICT programs is encouraging. The training arranged in collaboration with Ethiopian ICT Development Organization and Kennesaw State University of USA on principles of information security is one to be cited.

To put concisely, information security issue is not only a problem that technology can address alone but also a problem of a management to solve. Therefore, legal frameworks in the form of policy and standards are the most prerequisites to establish efficient and reliable cyber security systems. In line with this, Ethiopia has to do a lot yet to address the requirements for cyber security in the evolvement of information society.