LESOTHO TELECOMMUNICATIONS AUTHORITY

STATE OF CYBER SECURITY IN LESOTHO

June 2005-06-09

Prepared by Nthabiseng Pule

---

1. Country Background

Lesotho is a small country with a population of 1.8 million (Lesotho Bureau of Statistics 2003). It has a very low penetration of ICTs, generally. It is estimated that less than 1 percent of the population has access to the Internet (Ministry of Communications, Science & Technology 2005). Due to the low penetration of the Internet, and the fact that the Internet is not yet in the mainstream of business processes, cybersecurity is not an issue that is commonly discussed. Despite lack of discussions and perhaps awareness of the issue, Internet users in Lesotho are affected by spam and exposure to cyber fraud as users elsewhere.

2. Cybersecurity Issues

Currently, there is no legal framework regarding cybersecurity in Lesotho. There is, however, recognition by the government for the need to have a legal framework for electronic business. This is evidenced by inclusion of the subject in the ICT Policy of 2005. The policy itself is new, and its implementation is expected to take some time, also taking into consideration limitations such as skills and budget. So far, issues such as spam, electronic fraud, and privacy have not been addressed through legislation.

Spam is a real issue in Lesotho for both Internet service provider (ISPs) and users. Most of the spam comes from other countries, and as such is outside the jurisdiction of Lesotho. In Lesotho, there has been no case in court concerning spam. ISPs and corporate customers largely depend on technology to ensure security and they are aware that it would, in the majority of cases, to get perpetrators prosecuted in case of downtime they may suffer as a result of cybercrime.

ISPs often give their corporate customers basic information regarding how to minimise spam and avoid other problems that could be caused by the use of Internet for business. The ISPs also rely solely on technology to counter spam. Banks that provide Internet based services also try to make their customers aware of cybersecurity issues. However, it is not known how much awareness of this issues there is among Internet users in the country.

Local banks are introducing Internet based services, largely based on existing laws, and indemnifying themselves in areas not covered by such legislation. However, there has not yet been a case where the users of such services have been reported to suffer fraud through the use of such systems. Hence there is no precedent that could be used for future cases.

Due to close economic and social links with the Republic of South Africa (RSA), a number of people have personal and business banking accounts with South African Banks and most use the Internet banking services provided. In this case, the RSA legal framework for cybersecurity would be applied and any legal proceeding would have to take place in RSA.

Other issues relating to cyber security are the lack of technical and financial capacity to develop an appropriate legal framework, ensuring that enforcement agencies are well equipped to deal with cybercrime investigation and prosecution. Another important aspect that still needs to be developed is a base of people with technical skills to set and audit systems to ensure that they comply with relevant security standards. Only a few organisation can afford to pay for such expertise.

3. Conclusion

While cybersecurity may seem not to be a big problem in Lesotho at this time, it is expected to become a serious issue once more people have access to the Internet and businesses become more dependent on it for communications and e-commerce. Hence, it is important to have the necessary legal framework even at this early stage.

END