TRUST AND SECURITY

 Policy Brief

Security is listed as basic human right in Article 3 of the United Nations Declaration on Human Rights. Problems such as cyber security, data protection and content acquisition are becoming increasingly relevant in a world with an ever growing cyber space. This policy brief looks to address a select number of challenges faced in a Sri Lankan context.

**SUMMARY OF FINDINGS/ RECOMMENDATIONS**

1. Formulate an information security policy for the Government, as well as public and private institutions which handle public records
2. A secure centralized, online storage system to store personal documents.
3. Use of a two-step authentication process (using a one-time password (OTP)) when performing online transactions

**THE RESEARCH**

1. **METHOD**

Desk research was the primary method of collecting data. The existing legal framework and case studies conducted in the field of cyber security in Sri Lanka were perused. The Digital India initiative was also examined to draw policy recommendations.

1. **BACKGROUND**

Ten percent of the Sri Lankan population between the ages of 5 and 69 use the Internet (Department of Census and Statistics, 2014). The number of Internet and email subscribers was 3.4 million as at December 2014; this number has been rising at a CAGR of 35.7 percent over the past 3 years. (TRCSL, 2014) However this may not necessarily translate to a perceived increase in trust and security in the minds of the citizens,



Figure 1: Infection rates

Source: Microsoft Security Intelligence Report (2014)

Microsoft’s Security Intelligence Report suggests that computers in Sri Lanka encounter almost double the malware and potentially unwanted software in comparison to the worldwide rate.

1. **FINDINGS AND RECOMMENDATION**

**1. Formulate an information security policy for the Government, as well as public and private institutions which handle public records**The absence of a comprehensive security policy could lead to significant inefficiencies, as illustrated in the case study from the Computer Emergency Readiness Team (CERT)

A critical application run by a government department had become non-operational; the non-availability of the service had led to a loss in the productivity of the Department. The presence of a worm known as the CME-24 was identified on the application server. The CERT identified that this was because the Department’s network was not protected with up to date antivirus software. Furthermore, it was noted there was no security policy governing such security related procedures and actions.

A comprehensive security policy may prevent such occurrences. A minimum requirement for security policy could be specified. Recommendations may be made based on the International Organization for Standardization (ISO) code of practice for information security control.

**2.** **A secure centralized, online storage system to store documents**

A system could be implemented to reduce transaction costs related to locating and replacing document. A Digital Locker, similar to that implemented in India is recommended. The use of two separate folders are recommended in the Sri Lankan context;

1. A government document folder
2. A private document folder

The folder with government documents could contain documents including, but not limited to, a citizen’s birth certificates and examination results sheets. The documents would be watermarked and uploaded with a digital signature. Read only access would be given to the user to ensure retrieval on demand.
The second folder would operate much like Dropbox, except that the documents within the folder would be protected under Sri Lankan law. The data is private, and is only accessible to the government or other third parties by court order.

The uploaded content can only be shared with organizations which are registered with and specified by the system. The project could be implemented based on public-private key mechanisms. In both cases, the user would have the ability to select both the organization with which the documents would be shared and specify the documents which are to be shared. A private key is created with a customizable time durability; this can be shared with the desired organization; the user can create any number of custom keys and share it with various organizations. The said organizations would have access to the specified documents until the key expires. Each private key corresponds to a specific client’s public key and cannot be shared as a result.

**3.  Use of a two-step authentication process, using a one-time password (OTP) when performing online transactions**

Lax security standards when conducting online transactions could lead to grave losses.
The Criminal Investigation Department (CID) of Sri Lanka reported that banks holding Non Resident Foreign Currency (NRFC) accounts have suffered losses of over LKR 1 billion, due to illegal withdrawals using fake email addresses.

This problem may be resolved to a certain extent by using a two-step authentication process when transferring funds.

The research conducted indicates that only four banks are using a two-step authentication process (using an OTP) when carrying out online transactions at present.  It is recommended that all banks registered under the Central Bank Monetary Control System, which provide online banking service and facilitate online purchases should use such a process.

**SOURCES**

* Department of Census and Statistics (2014) Computer Statistics 2014. Retrieved from <http://www.statistics.gov.lk/ComputerLiterarcy/BuletinComputerLiteracy.pdf>
* Telecommunications Regulatory Commission of Sri Lanka (2014) Statistical Overview, December 2014, December 2012
* International Organization for Standardization (2013) ISO/IEC 27002: 2013, retrieved from <https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en>
* Computer Emergency Relief Team, Case Study- the Worm. Retrieved from <http://www.cert.gov.lk/caseStudies.php>
* Central Bank of Sri Lanka (2015) Guidelines on Opening New Banks in Sri Lanka, retrieved from <http://www.cbsl.gov.lk/pics_n_docs/09_lr/_docs/licensing/bsd_licensing.pdf>

**AUTHOR/S**

Gayani Hurulle| LIRNEasia| gayani@lirneasia.net | +94 (77) 3339727

Shafny Mahir | Faculty of Information Technology, University of Moratuwa | shafny@gmail.com | +94 (77) 34151163

Santhusha Jayatillaka | Nisala Nenasela | santhshaj@gmail.com | +94 (71) 6414854