CYBERWELLNESS PROFILE SAINT VINCENT AND THE GRENADINES

BACKGROUND

Total Population: 109 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 52.00%
(data source: ITU Statistics, December 2012)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Saint Vincent and the Grenadines does not have any officially recognized criminal legislation pertaining to cybercrime.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation to cybersecurity has been enacted through the following instruments:

- Electronic Transaction Act
- Electronic Evidence Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

There is no available information regarding any officially recognized national CIRT in Saint Vincent and the Grenadines. A CIRT readiness assessment was conducted for Saint Vincent and the Grenadines by the ITU in 2012.

1.2.2 STANDARDS

There is no available information concerning any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no available information concerning any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

There is no available information concerning any officially recognized national cybersecurity strategy in Saint Vincent and the Grenadines.

1.3.2 ROADMAP FOR GOVERNANCE

There is no available information concerning any officially recognized national governance roadmap for cybersecurity in in Saint Vincent and the Grenadines.

1.3.3 RESPONSIBLE AGENCY

The lead agency for cybersecurity in Saint Vincent and the Grenadines is the SVG Police Force, which has created an Information Technology Unit to oversee and support the investigation of all cybercrime and information security-

related matters and thus is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

There is no available information regarding any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no available information regarding any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

There is no available information regarding any officially recognized sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information regarding the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

There is no available information regarding any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

International cooperation has centered largely on solicitation of support when needed from the experts of the Cyber Forensic Laboratory in Antigua and Barbuda.

1.5.2 INTRA-AGENCY COOPERATION

There is no available information concerning any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no available information concerning any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Saint Vincent and the Grenadines is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

Personnel from the government's Technology Unit have also participated in cybersecurity and cybercrime related training offered by regional and international partners including the OAS, US Department of State (DS/ATA), CTU, and INTERPOL, among others.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION AND STRATEGY

Specific legislation on child protection has been enacted through the following instruments:
- Section 71 and 73 from the Electronic Transactions Act.

2.2 UN CONVENTION AND PROTOCOL

Saint Vincent and the Grenadines has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.
Saint Vincent and the Grenadines has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

Saint Vincent and the Grenadines does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Saint Vincent and the Grenadines does not have an officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.
