Cybersecurity Strategy in Developing Nations: A Jamaica Case Study

Kevin P. Newmeyer, Ph.D.

Abstract

Developing nations have been slow to develop and implement cybersecurity strategies despite a growing threat to governance and public security. This qualitative case study examined how the government and private sector in Jamaica viewed the state of cybersecurity in the country, and how the country was developing policy to respond to cyber threats.

Problem

At the time of the study in late 2013, Jamaica had not published a **national cybersecurity strategy**, even though the most recent national security strategy cited cybercrime as a major threat (Clayton, 2012).

Like other Caribbean leaders, the Government of Jamaica tended to have a **narrow view of cybersecurity** as an ID or credit card theft problem and failed to account for threats to critical infrastructure or challenges to national security.

Although the country had cybercrime legislation, **enforcement was limited** and suffered from lack of knowledge and cooperation domestically and internationally.

Purpose

The purpose of the study was to develop insights into cybersecurity policy development and cybersecurity strategy implementation in Jamaica, which may provide insights for other nations in the region.

I used the study to answer questions about what policy and strategy options emerging globally can a developing Caribbean nation, such as Jamaica, adopt or adapt to improve cybersecurity for its citizens and nation. The reply needed to be given in the context of size, economy, and public-private relations applicable to the region and not merely imported from outside.

Relevant Literature

Since 2001, there is a growing body of literature on national cybersecurity strategy, which is at present aimed largely at the more highly developed nations.

Cole et al. (2008), Tagert (2010), and Phahamohlaka et al. (2011) found that the models proposed by the developed West and the international organizations prior to their studies failed to meet the needs of developing African nations.

Other scholars found that even among the developed nations, there was a need to tailor cybersecurity strategies to the political and cultural realities of individual nations (Falessi et al. 2012; Klimberg, 2012; Luiijf et al., 2013).

The national security (Harknett & Stever, 2009, 2011) economic (Moore, 2009; Van Eeten & Bauer, 2009), and public health (Charney 2012, Mulligan & Schneider, 2012; Rosenzweig, 2011) approaches to cybersecurity were examined for applicability.

Cybersecurity strategies from Colombia (2011), Panama (2013), and Trinidad and Tobago (2012) provided regional context for comparison.

Research Questions

RQ1 - How do the government and private sector in Jamaica view the state of cybersecurity in the country?

RQ1 - How is the Government of Jamaica currently developing and implementing policy to respond to cyber threats?

RQ1 - What additional measures and policies could the Government of Jamaica implement to incorporate international best practices in national cybersecurity policy?

Procedures

This research was a qualitative case study.

Document review of legislation and commentary prior to arrival.

Purposeful sample of government, private sector, and academia.

Government participants from military, police, and technology ministry.

Private sector included telcoms, consultants, and media

Field work in Dec 13 for 7 interviews face-to- face supplemented by 6 email interviews using a ten question researcher developed protocol

Additional policy documents obtained from interview participants provided insights on the ongoing policy process

Data Analysis

An iterative and repetitive process was used to analyze the data. **Atlas.ti** software supported visualization of data.

Findings

There is an **emerging international consensus** on what national cybersecurity strategy should include.

Cybersecurity policy was being developed in Jamaica but the **process was far from complete**.

Elements of National Cybersecurity Strategy

Top level government support	National Cybersecurity Coordinator	National Focal Point Organization	Legal Framework	International Cooperation
Cybersecurity Awareness Education	Public-Private Cooperation	Multi-stakeholder approach	Civil Liberties protections	CSIRT/CERT
Risk Assessment Process	Identify Critical Infrastructure	Technical Guidelines	Cyber exercise and contingency plans	Cybersecurity Workforce Skills Training

Limitations

The case study was limited to one nation at a given point in time.

The study involved a limited number of participants

Although the specific findings are limited to Jamaica, some generalizations are possible.

There is a lack of good data collection on cyber incidents in Jamaica

Conclusions

The study included specific recommendations for the Government of Jamaica to include in their developing national cybersecurity strategy.

The nation needs to develop a Computer Emergency Response Team (CERT) as soon as possible.

The Ministry of Education in Jamaica needs to be more involved in cyber strategy development and implementation.

Social Change Implications

The insights from this study could improve the capacity of Jamaica to confront a series of threats to its security and economy

A **robust cybersecurity security strategy would better position the nation** to reap the rewards of an Internet-enabled economy and to help it overcome the digital divide.

A national cybersecurity strategy that addresses the emerging international best practices identified in this study will add to growth and positive social change.

The William J. Perry Center for Hemispheric Defense Studies provided funding to support fieldwork.
*Dissertation Committee: **Dr. Christopher Jones, Dr. Dwight Toavs,** and **Dr. Gema Hernandez***