Chapter 2
The Development of Cybersecurity Policy and Legislative Landscape in Latin America and Caribbean States

Indianna D. Minto-Coy
University of the West Indies, Jamaica

M. Georgia Gibson Henlin
Henlin Gibson Henlin, Attorneys-at-Law, Jamaica

ABSTRACT

The rise and evolution of telecommunications networks over the last few decades have brought immeasurable benefits. Attention to the negative side of these developments has been slow, particularly in the Small Island Developing States of the Caribbean where countries are slowly becoming aware of the developmental, social and economic challenges posed by cybercrimes. Attention has largely been on developed states. However, the experiences covered here add to the global picture on the state of cyber security, increasing understanding of alternative experiences and where they sit alongside the more popular ones such as the US. The chapter details some major development in cyber security in the Caribbean, examining the development of the legal, institutional and organizational landscape in response to growing internal and external cyber threats. Main players and efforts are identified. Information was gathered from interviews and content analysis and the authors' first-hand knowledge.

DOI: 10.4018/978-1-5225-1941-6.ch002

INTRODUCTION

The rise and evolution of telecommunications networks over the last few decades have brought immeasurable benefits to the global economy. The use of the Internet via mobile devices has grown as a tool for innovation and entrepreneurship. This is seen for instance in the proliferation of e-commerce, e-government, social networks and chat sites and the convergence of mobile and telephone technologies with sectors such as banking. This is influenced by the price of access, which is trending downward for most of the world's populations. The economic opportunities that have been created are significant and will continue to be the case, as ICTs and telecommunications continue to be the backbone for businesses and everyday interaction in an increasingly networked global landscape.

Initial inattention to cyber risks and security challenges consequent on these innovations is decreasing. For the most part however, these are still reactive to cyber threats. The reality is that the technologies are not only still emerging but also rapidly changing such that it is difficult to grasp or analyse their full risk profile or effect. The security challenges also arise from the manner in which the Internet is used and on what media. The preferred media appears to be mobile devices. Each mobile device, for example, comes with security or privacy preferences. Some persons inadvertently activate applications that gives access to their location or information, unknowingly allowing their every movement to be tracked.

Cyber security threats include, the interception of data, harassment and cyber stalking, unauthorised access to or theft of computers, the commission of sexual offences online, criminal copyright infringements, and disruption of critical national infrastructure. In fact, most reported threats are external, such as phishing. This is based on anecdotal evidence from banks and attorneys. The banks send out regular warnings to their customers not to disclose their personal information in response to emails requiring them to do so as they would not request such information by that medium. Attorneys very often receive letters similar to the Nigerian 419 phishing scams requesting them to do work but a resistance to paying the retainer as requested. It is therefore not unusual to see the websites of mostly banks warning their customers of the dangers of "phishing and internet scams". As such, while the lives of citizens have been made easier, the Internet has also increased avenues for the exploitation of technology for criminal ends. With more interaction being facilitated through the Internet and more people than ever before being connected virtually, the threats not only have an adverse effect at the individual level but also for governments, non-governmental organisations and businesses locally and globally.

A number of tools have emerged to enable cybercrimes and these have grown in sophistication over the years. These include, the Blackhole Exploit Kit, which is targeted at computers. However, an increasing number of these tools are targeting

What and Where are the Risks of International Terrorist Attacks: A Descriptive Study of the Evidence

Kenneth David Strangand Serafina Alamieyeseigha (2015). *International Journal of Risk and Contingency Management (pp. 1-20).*
www.irma-international.org/article/what-and-where-are-the-risks-of-international-terrorist-attacks/127538