

Cyber security and the Caribbean

MOST Caribbean Governments and companies have yet to take seriously the threat posed by cyber attack. This is despite signs that the region is not immune to the actions of those who use the Internet to breach national security, undertake criminal activity or behave maliciously.

Just a matter of weeks ago, LIME Barbados' broadband network came under a denial of service attack. Typically, in such an intrusion, the attacker tries to prevent legitimate users from accessing or utilising a particular service by launching a flood of traffic from multiple points in a manner that slows speeds or brings a system down.

According to the company, large numbers of customers experienced degradation in their broadband service as a result of the attack on the company's Internet infrastructure from an external source. Though confined to a small portion of LIME's Internet customer base, the attacker gave the appearance of a having a wide scale impact on the company's network.

LIME said that its servers had not been compromised and that it had increased its defences both locally and internationally. It also stated that it was the company's intention, if the source could be identified, to consider legal action against this type of Internet criminality.

There are also other recent examples. According to the informative and thought provoking Caribbean web blog, ICT Pulse, which discusses topical ICT issues from a Caribbean perspective, a presenter at last year's Caribbean Internet Governance Forum, suggested that hackers had breached the websites of several Chambers of Commerce in the region; that the systems of almost all banks in the region had been hacked, and many of them more than once; and a major Caribbean airline had also come under at-



The View from Europe

by David Jessop

tack. In a further examples, a local Dominican Republic activist group recently deprived newspaper readers of access to one of the country's leading newspapers for some hours, apparently in pursuit of anti-capitalist aims. There are also unconfirmed reports that the Trinidad and St Maarten government's systems have been compromised and confidential documents and emails stolen and leaked.

What is surprising is that the issue is not being taken more seriously as the region's relatively fragile infrastructure makes whole economies particularly vulnerable. For the most part, governments and security agencies in the region seem not to have considered in any depth this vulnerability and its implications or developed detailed planning to respond to any serious attack.

This is surprising as the Caribbean is one of the world's fastest growing regions for Internet usage. It has, over the last five to ten years, become reliant on maintaining digital communications for services for everything from national security, through to the support required for financial services centres, commerce and day to day communications. The region is also the location of some internationally important communications

hubs. According to Internet World Stats some 28.7 per cent of the Caribbean population now use the Internet or some 11.9m users out of a total Caribbean population of 41.4m people. The countries within the largest penetration as a percentage of population are St Lucia at 88.5 per cent of the population, St Vincent, 73.2 per cent; the Cayman Islands, 72.2 per cent; and Jamaica, 55.1 per cent, although in absolute terms it is unsurprisingly the more populous nations such as the Dominican Republic and Puerto Rico that record the highest number of users.

These high usage figures are paralleled by the number of cell phones with some statistics suggesting that mobile phone use in the Caribbean now approaches 70 per cent of the population and significant numbers for usage of social media such as Twitter and Facebook with a parallel growth in apps, some of which may eventually be linked to banking and commercial translations.

All of which is a very good reason to emphasise the need to give cyber security and cyber crime much greater national and regional attention.

Recently, the Organisation of American States Secretary General, Jose Miguel Insulza, when opening a meeting 'Strengthening Cyber Security in the Americas' highlighted the need to give greater consideration to this issue. What was required he suggested was the development of a modern view of co-operation between the public and private sectors, since the latter owned and operated most of the information infrastructure on which the countries of the Americas depend. His view was reflected by international experts. Making a special presentation to the forum, the Director of International Cyber Policy at the United

SECURITY on Page 11

Legislation necessary to address cyber crimes

SECURITY **from Page 10**

Kingdom Foreign and Commonwealth Office made clear that the response to cyber terrorism was to develop much closer collaboration between public and private sectors, a process successfully undertaken in the UK.

Unfortunately, while legal redress may be talked about, few Caribbean jurisdictions have the necessary legislation, regulations or infrastructure to address cybercrimes making it punishable to violate a network.

It is also far from clear whether regional law enforcement agencies have the legal cover to co-operate with external government agencies in this area, given that most

cyber crimes are extra-territorial in their effect.

AS ICT Pulse notes, the Caribbean has become so focussed on ensuring Internet access and improved connectivity, that the region has not placed the same level of effort on implementing systems to protect networks and information.

Policy

They argue that what is required is a Caribbean Internet Governance Policy Framework.

In a region in which it sometimes feels like Ministers and officials are just catching up with the economic and strategic significance of tourism, suggesting a public debate on what the region or individual nations need to do in the context of cyber security

might be considered eccentric.

Regulation

However, it should be clear that the future economic development of the region requires not just a modern communications infrastructure and high speed networks, but also the necessary regulation, legislation, enforcement and policing.

Without this it is hard to see how any Caribbean nation can argue that the region is a sensible location for investment.

(David Jessop is the Director of the Caribbean Council and can be contacted at david.jessop@caribbean-council.org Previous columns can be found at www.caribbean-council.org)

