The View from Europe
By David Jessop

More action required on cyber security

Two years ago I suggested in this column that few Caribbean Governments or companies were taking seriously the threat posed by cyber attack and cyber crime. This was despite evidence to suggest that the region was increasingly subject to damage by those who use the internet to breach national security, undertake criminal activity or behave maliciously.

At the time I noted that the future economic development of the region required not just a modern communications infrastructure and high speed networks, but also their regulation, appropriate legislation, and its enforcement and policing. Without this, I commented, it was hard to see how any Caribbean nation can argue that the region is a sensible location for investment.

Since then the issue has taken on all sorts of different dimensions.

At one end of the spectrum there has been the disclosure by Edward Snowden, a former National Security Agency contractor, that the US, and by extension most other developed nations, were mining data on an industrial scale, principally in an attempt to secure all countries against terrorism. At the other, and far more intrusively, big search engines, internet providers and companies were combining data from every individual's web searches, supermarket purchases, hotels and hundreds of other sources, and then selling on information about the specific interests of individuals in order to target products or services at them.

More specifically, in the Caribbean, there have been sporadic but alarming reports about security breaches by hackers at banks and companies as a result of which credit card details have been stolen, denial of service attacks have taken place on telecommunications providers and companies, government files have been electronically removed, and the suggestion has been made that offshore centres could be used remotely to facilitate such activities.

Only relatively recently has the issue been taken more seriously as the region has slowly come to understand that its fragile infrastructure makes it particularly vulnerable. As a consequence governments, security agencies and companies in the region have begun to consider in any depth, their national financial, economic or political vulnerability, and undertake detailed planning on how to respond to a serious attack.

Recent commentaries in the excellent, informative and thought provoking Caribbean web blog, ICT Pulse, which discusses topical ICT issues from a Caribbean perspective, quotes Bevil Wooding, who heads the volunteer Caribbean Network Operators Group (CaribNOG), as saying that people mistakenly believe that emerging markets like the Caribbean, with relatively small economies, are less likely to be a target of attacks. "In reality, it is quite the opposite. Regions like the Caribbean, precisely because of their underdeveloped legal frameworks and limited capacity to detect or investigate, are now very attractive locations for hackers and cybercriminals to focus their activities," he is quoted as saying.

This and other remarks by industry experts and international bodies such as the Organisation of American States suggest that there is an urgent need for action in a number of areas.

Firstly in relation to the law: most Caribbean nations do not yet have any let alone modern legislation against electronic crimes. While legal redress may be talked about, all Caribbean jurisdictions need 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 extraterritorial.

Secondly, there needs to be a rapid growth in trusted Caribbean companies of the kind that are emerging in Barbados, Trinidad and Jamaica with outreach to international expertise able to undertake vulnerability assessments, penetration testing, compliance and security awareness training.

Thirdly, it requires levels of public and private sector co-operation of a kind not normal in much of the Caribbean, to develop systems, secure forms of information exchange and regular consensus-based dialogue as these are issues that touch on the viability of nations as well as individual enterprises and research.

Fourthly, there should be programmes specifically aimed at the banking, finance and tourism sectors which are particularly vulnerable both reputationally and from the perspective that damage caused can have an adverse reputational and economic effect for years to come on a brand or a product.

Fifthly, it requires some of the important initiatives being considered or being developed by some regional governments to become the subject of broader inter-regional and hemispheric co-operation as, by definition, the threat crosses all boundaries.

And sixthly, it is vital that home grown companies able to support IT security are encouraged, as it is clear that it is more appropriate that issues that are about national sovereignty and national interest should be entrusted to local bodies with capability and that understand best the operating environment in the region in which they are located.

The Caribbean is one of the world's fastest growing regions for internet usage, having become over the last five to ten years reliant on maintaining digital communications for services for everything from the support required for financial services centres, to commerce and day-to-day communications. It is also the location of some internationally important communications hubs.

It has, according to Internet World Stats, very high internet penetration with some 28.7 per cent of the Caribbean population using the internet or some 11.9m users out of a total Caribbean population of 41.4m people; figures are exceeded by the number of cell phones in use, which some statistics suggest are now owned by 70 per cent of the population with a parallel growth in apps, some of which may eventually be linked to banking and commercial translations.

What is clear is that the level and intensity of cyber attacks is increasing and that cyber crime is not just an issue for developed countries.

Experts suggest that future attacks will increasingly be directed to softer targets in locations like the Caribbean not least because they are regions through which huge sums of money flow electronically for tax efficiency or advantage and because of its infrastructure links to the United States and Europe.

It is time for more attention to be paid to cyber security.

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
January 12, 2014