Summary of Issues and Outcomes

5th National Cyber Security Conference, MICT, CARIMAC, UWI

November 28 & 29, 2017

- The Conference called on the Government of Jamaica to expedite the passage of the proposed Data Protection Act, especially in the context of the government's planned introduction of the National Identification System (NIDS). This call for the passage of a Data Protection Act, has been made at successive previous conferences. It was noted that while a draft of the Act was now before a Joint Select Committee of the Jamaican Parliament, the DPA should have been passed before the November 2017 passage of NIDS, in order to afford citizens better protection for the personal and biometric data that will be collected on them as part of NIDS.
- As a key part of measures to enhance Cyber security, both private and public sector organizations and MSME should step up training in the areas of financial literacy, technological literacy and cyber security among all age groups.
- The conference heard of new cyber security approaches, described as 'post-quantum' to safeguard the vulnerable. Consideration should be given to an approach to cyber security which focused more on protecting data rather than primarily targeting the devices. Prediction that this will be the dominant approach in five years.
- It was suggested that the focus and language should be cyber-defence rather than cyber-security. Use of the term defence suggests a proactive rather than reactive outlook.
- In an era of the Internet of Things (IOT) in which connected devices are conduits of cyber risks, a new concern is safeguarding against what was described as an emerging "ransomware of things". Security and defence measures are needed for smart devices, tech gadgets and connected domestic appliances that collect and store data. We will need to be especially aware of our vulnerabilities from these devices.
- The conference was again reminded of the need to focus on "fleshware" (the employees or people in general that use the technology). The term and issue came up at last year's conference. Internal staff can be a security threat, so frequent security screening is necessary. It was reaffirmed that all users should be efficiently trained in cyber security and data defence measures, ranging from use of strong passwords, regularly changing passcodes, to institutional cyber audits and penetration testing.
- UWI and other educational institutions should consider provision of cyber security courses and certification as a requirement for employees to work at certain levels.
- In order to enhance the services offered especially to small businesses locally and regionally, the idea of developing managed shared services and joint IT Support Centres. These can be especially tailored to serve varied types of MSME, ranging from attorneys to small youth startups.

- Technology is the new competition that is driving innovation and driving down costs. Disruptive Innovation is serving the under-served. All banks are currently at risk of losing consumers to more innovation and disruptive providers such as cryptocurrencies and mobile money. Established businesses such as banks as well as all service providers should therefore explore new solutions that are more heavily customer-focused and mobile.
- The time and cost of transferring money have been reduced tremendously. Intermediates are being discarded. There is the question as to the future of middle-players. Institutions and business must get ready for an era that was described as one of 'disintermediation', or operating without too many middle players.
- Better and more clearly explained notification about the implications of the use of apps is needed. Too often apps are offered that are designed to steal data or to be intrusive. Persons and institutions should be aware of where data go, how the data are used, and the routes to opting out of certain applications or conditions.
- The issue of TRUST remains at the centre of people's attitude to technology use and security. One area where this issue looms large is in electoral processes. Can we trust technologies that aid in the carrying out of voting or voter verification? The pervasive influence of computational propaganda which employs media tools such as "bots" and "fake news" are identifiable threats to the electoral and democratic process. It was recommended that relevant agencies should convene public forums and educational sessions to inform citizens about risks, including in the supply of their news and public information as well as the regulation of media (online space).
- Greater research and caution were recommended in any high value investment in or widescale adoption of emerging crypto-currencies. However, low level initial investment and more careful experimentation in their use was recommended, even while Caribbean institutions should continue to explore Fintech and related new ways of transacting business. The academic institutions, central banks and other agencies should more closely research and examine such innovations as blockchain and all aspects of Fintech (financial technology) in order to not be left behind in major developments worldwide.