Regulatory, Policy and Legislative Issues in countering Cyber Crimes

Robin M. Sykes

Chief Technical Director

Financial Investigations Division

4th National Cyber-Security Conference

29 November 2016

The Cybercrime Framework in Jamaica

- The Cyber Crimes Act
- Regulatory Statutes such as the Banking Services Act, the Securities Act, Insurance Act, etc.
- General criminal statutes, notably the Proceeds of Crimes Act, Law Reform (Fraudulent Transactions) Act;
- Role of the Communications Forensics and Cyber-Crimes Unit of JCF;
- Role of Cyber Incident Response Team;
- Role of the Private Sector;
- Role of Regulators;
- Role of specialized agencies such as the Financial investigations Division

How ready is the framework for 21st century cyber-crime?

- Malware/Ransomware Attacks
- Hacking Attacks That Release Confidential Data
- Phishing And Other Fraudulent Attacks;
- Cyber Bullying And Extortion;
- Child Pornography And Human Trafficking;
- Identity Theft And Related Activity;
- Recruitment and incitement of terrorism over the internet;
- Dark Web: sales of weapons, services , etc.

APART FROM EXPRESS CRIMINALITY…

- There are modern developments that have a massive capacity to do good (particularly from a financial inclusion standpoint) but also have the capacity to be misused for criminal activity;
- Cyber/crypto currencies, new payment methods all have a potential for opening up financial services to a wider population but also have the potential for misuse;
- The question is how should they be regulated in a risk based approach without stifling innovation.

Law Enforcement Side: The Cybercrimes Act 2015

- Creates a number of offences:
- S. 3. Unauthorized access to computer programme or data;
- S. 4 Access with intent to commit/facilitate commission of offence;
- S. 5 Unauthorized modification of computer program or data
- S. 6 Unauthorized interception of computer function or service;
- S. 7 Unauthorized obstruction of operation of a computer;
- S. 8 Computer related Fraud or forgery
- S. 9. Use of computer for malicious communication;
- S. 10 Unlawfully making device available for commission of offence
- S. 11 Offences relating to protected computers (GOJ/LEA/Infrastructure/ Banking and financial services/Utilities/ computers)
- S. 12 Inchoate offences (Accessories, Aiding and Abetting)
- S. 13 offences prejudicing investigations;
- S. 14 Offences by bodies corporate

Cybercrimes Act: Investigative Provisions

- Section 14 power to issue a notice for a person to preserve data;
- Section 15 search and seizure warrants;
- Section 16 record of material seized must be maintained, copy provided if requested;
- Section 17 court may grant production orders in relation to material that’s relevant to an investigation.

Further provisions

- S. 19 Regulations to be issued;
- S. 21 Provisions to be reviewed by a joint select committee within 2 years of March 2010.
- **Comments:**
- What's the scope of "unauthorized access"? Does it include "ethical hacking"? What about LEA interference with a computer for criminal disruption purposes?
- Does the Act give LEAs the strong powers necessary to combat Cyber-Crime? UK now has the Investigatory Powers Act 2016 (a step too far?)
- What will be the impact of the privacy provisions of the Constitution and the proposed Data Privacy laws?

Interception of Communications Act

- S. 3. Allows a judge to issue a warrant to permit the interception of communication in the course of its transmission by an authorized officer.
- Must prove that the warrant is necessary for national security, for the detection of certain offences in the Schedule, other means oif investigation unlikely to be successful, too dangerous or impracticable and its in the best interest of the administration of justice;
- S. 6. Warrant can be issued for up to 90 days. Can be renewed for another 90 days.
- S. 10 specifies duties on providers to take steps to ensure that it may provide assistance to comply with such warrants;
- S 11 gives power to judge to specify conditions of confidentiality of intercepted communications;
- S 12 give officer authority to apply to judge for the key (code password, algorithm that allows access) to a communication

Elements of the Law Reform (Fraudulent Transactions) (Special Measures) Act)

- S. 6 Offence of using an access device (card, plate, code access number, PIN other means to obtain a benefit or effect a transfer) to transfer or transport money in or out of Jamaica;
- S. 8 Offence relating to theft, forgery of access device;
- S. 9 making repairing selling exporting importing possessing instrument device for copying data from access device or forging an access device;
- S. 10 offence of knowingly obtaining or possessing transmitting distributing identity information in circumstances where there is a reasonable inference that information has been used or is intended to be used to commit an offence under this Act or any other law.

The Players: JCF Communications Forensics and Cybercrime Division (CFCU)

- Currently 28 officers; 80 considered to be optimal.
- Internet Forensics Unit: Cybercrime, Social media Forensics, Electronic Fraud Analysis & Investigations, Cyber Incident Response and Investigative support;
- Digital Forensics Laboratory: Mobile, computer, video and audio forensics, Network forensics and ICT and network management;
- Communications Forensics Analysis: special projects and Intell analysis, Communications Analysis, cell site survey, Communications service provider liaison
- Administration and Quality Control

The Financial Investigations Division

- Houses both investigators as well as the Financial Intelligence Unit focussed on tracking the finances of persons committing financial crime (within Jamaica) of which cybercrime is a subset.
- The FIU receives and analyses a variety of reports from the financial sector relating to suspicious transactions, transactions under the Terrorism Prevention Act, etc.
- The FIU has access to counterpart FIUs globally for the sharing of financial intelligence through the Egmont Network of Financial intelligence Units.
- The FID works alongside the primary investigators CFCU to carry out financial investigations alongside the investigations for the predicate offence. We use tools such as criminal forfeiture (post conviction), civil recovery and cash seizures to access the funds or property.
- Fid is building its own cyber-forensics capacity with respect to the management of digital evidence obtained in operations.

In practice

- The revised Cyber law is new, although there have been conviction (recent case involving transient individuals who were using skimming equipment);
- Cyber forensics critical to the Cartel case and proved the ability of JCF and ODPP to successfully manage that evidence.
- The resource issue for the CFCU must be addressed to allow that Unit the capacity handle the myriad of uplifted computers and phones that a common feature of law enforcement activities (especially lottery scam cases).

On the policy front

- The key focus has to be on vigilance and prevention as a fundamental to cyber-risk prevention.
- The GOJ under the National Cyber Security Strategy is a fundamental tool in formulating and establishing a co-ordinated approach to this issue
- The NCSS established the Cyber Incident Response team;
- Services to include incident response, handling and co-ordination, vulnerability response and co-ordination, alerts and warnings, threat analysis, security audits and assessments, forensics and risk analysis education and training.

Private Sector & Regulators

- The Private sector has a vested interest in protecting their operations as well as the transactions of their customers and make massive investments in this regard;
- The Supervisors have a role in testing the systems of their regulated entities in order to form a view on the robustness of their systems.
- The Banking Services Act also has obligations for customer confidentiality that carry criminal penalties.
- Again do regulators have the resources and capacity to meaningfully carry out these assessments?

Regulators have an additional role in the design of the architecture for future financial services

- The Bank of Jamaica is the driving force behind Jamaica’s National Financial Inclusion Strategy;
- Currently engaged in research as to potential adjustments in the framework for AML/CFT that will allow for simplified due diligence for lower risk inclusion products as well as methodologies for the technical assessment of risks in different “*inclusion*” products in order to determine whether they will qualify for low risk/simplified due diligence treatment.

Digital/Cyber Currencies

- The BOJ is in discussion with some promoters;
- Banking Services Act defines "banking business" as (iv) the issue of electronic money;
- S. 10 prohibits the conduct of banking business unless you are licensed under the Act.

Electronic Money

- Electronic money means monetary value represented by a claim on the issuer therreof, which value is –
- (a) stored or recorded by electronic means;
- (b) provided by the issuer in exchange for the present or future receipt of monies or other valuable consideration from the person entitled to make the claim;
- (c) transferrable and accepted as a mean of payment by persons other than the issuer whethjer via point of sale or similar technology or otherwise;
- (d) Redeemable or repayable in full or in part on demand for cash by deposit into a bank account or through the use of any automated banking or automated teller machine or any other similar device; or
- Not referable to credit facilities whether secured or unsecured extended by the issuer.

Conclusion

- Many different developments on the landscape;
- The threat is growing and the obstacles include lack of resources and capacity;
- According to the 2016 IDB Report on Cyber Security Preparedness in Latin America and the Caribbean, Jamaica has a few areas where we have reached an established level of cyber security maturity (policy, legislation, law enforcement) but have not reached a strategic or dynamic level of cyber-security in any of the 49 Cyber Security Capacity Maturity indicators.
- The question is how will we strengthen the framework using our limited resources in a meaningful way.