Cybercrime
Research Institute

ICT LEGISLATION AND THE IMPACT ON E-COMMERCE IN BARBADOS

ITU Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (HIPCAR)

Stakeholder Validation and Capacity Building Workshop

5-6 September 2011, Barbados

Prof. Dr. Marco Gercke

Cybercrime
Research Institute

CREDITS

This document has been produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union

Cybercrime
Research Institute

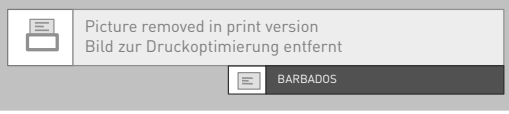
TOPICS FOR TODAY

- E-Evidence
- Cybercrime
- Interception
- Impact for E-Commerce
- Why harmonisation is important (HIPCAR)
- Advantages for a small island

Cybercrime
Research Institute

E-COMMERCE BARBADOS

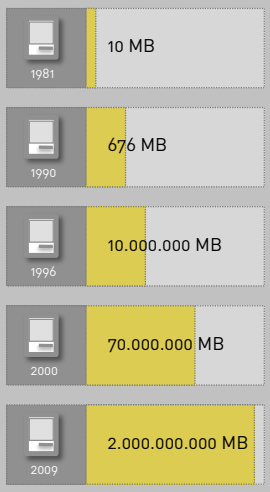
- E-Commerce offers unique opportunities for small and developing countries
- The situation is similar in Barbados
- E-Commerce offers local businesses new opportunities
- Especially relevant for the tourism sector
- In order to fully benefit from those advantages a legal framework is essential



Cybercrime
Research Institute

DIGITAL DATA

- One explanation for the emerging importance of digital evidence is the fact that the number of digital documents are intensively increasing
- Costs for storing one MB of data was constantly decreasing during the last decades
- Today it is cheaper to store information digitally than to keep physical copies



Cybercrime
Research Institute

E-MAIL FORENSICS

- More and more correspondence is done electronically
- Uses of Internet-services such as e-mail leave various traces
- Information contained in an e-mail go way beyond sender, recipient, subject and content
- Header information can help law enforcement to identify the sender of threatening mails

Picture removed in print version
Bild zur Druckoptimierung entfernt
E-MAIL FORENSICS

Cybercrime
Research Institute

ALTERATION

- As valuable e-mails can be for an investigation as important it is to keep in mind that e-mails are only text documents
- Open to alteration
- Courts in some jurisdictions are therefore restrictive when it comes to the admissibility of electronic mails

Picture removed in print version
Bild zur Druckoptimierung entfernt

ALTERATION OF A MAIL

Cybercrime
Research Institute

BACKGROUND

- Emerging relevance of digital evidence influences the procedures in court
- It is possible to divide between two different processes:
  1. Substitution of traditional evidence by digital evidence
  2. Introduction of digital evidence as additional evidence
- Influence is not limited to the fact that courts need to deal with digital evidence
- Even the design of courtrooms is influenced

Cybercrime
Research Institute

CYBERCRIME

Cybercrime
Research Institute

CYBERCRIME

- Cybercrime is a truly global phenomenon
- The ability to fight Cybercrime is not only relevant for countries that host offenders
- Today the majority of Internet users are based in developing countries
- With a national WIFI project even more users will be connected
- In order to protect those users law enforcement needs to be able to fight against Cybercrime

Cybercrime
Research Institute

ILLEGAL DATA AQUISITION

- Business secrets and customer information can be of great relevance for competitors and crime groups
- As today information are mainly stored electronically such information can rather easily be copied and distributed
- Recent studies indicate an increasing risk of "insider attacks"

Cybercrime
Research Institute

ILLEGAL DATA AQUISITION

- Data breaches can have a negative impact on companies reputation
- Both internal anti-cybercrime strategies as well as cooperation with law enforcement can therefore be crucial for businesses

Cybercrime
Research Institute

DECENTRALISED SERVICES

- Popularity of network based service increased the threats
- Availability of high-speed Internet connections and server infrastructure today enables the development of storage concepts that are not anymore based on local but decentralised storage
- „cloud computing“ and „cloud storage“

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE: AMAZON CLOUD COMPUTING

Cybercrime
Research Institute

ILLEGAL ACCESS

- Another reason for increasing threats is the popularity of wireless Internet devices
- Wireless technology (WLAN / WIFI) is a popular technology to make services available in a local area

Cybercrime
Research Institute

ILLEGAL ACCESS / INTERCEPTION

- Many Internet users that set up wireless access devices are not aware that the related signals are available in a radius of up to 100 meter
- Offenders can make use of the internet connection from the distance to commit crimes

Cybercrime
Research Institute

ILLEGAL ACCESS

- War Driving
- Unlike classic hacking "war driving" is not aiming for a certain victim but for any vulnerable system
- searching for wireless networks by moving vehicles
- „Useful" to hide the identity of the acting person

Cybercrime
Research Institute

DEFAMATION

- In addition to defamation the Internet is used to publish wrong information about businesses and blackmail them

Cybercrime
Research Institute

DATA INTERFERENCE

- The term data interference is used to describe a negative interaction with regard to computer data
- Example: Computer virus that deletes information on a hard drive
- A computer virus is a malicious software that is able to replicate itself and infect a computer without the permission of the user in order to carry out operations
- Primary target: Computer data

Cybercrime
Research Institute

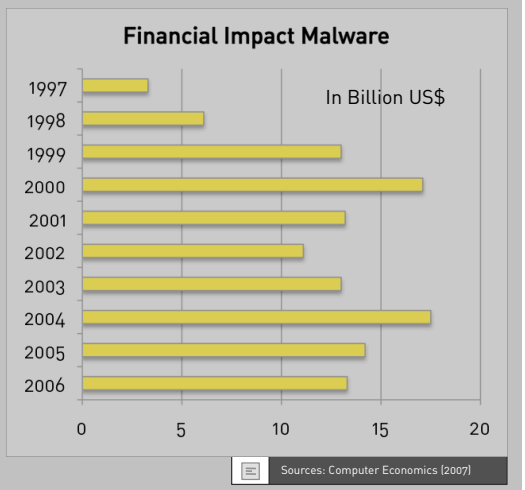
DIGITAL DATA

- Emerging importance of digital information
- Number of digital documents is intensively increasing
- Costs for storing one MB of data was constantly decreasing during the last decades
- Today it is cheaper to store information digitally than to keep physical copies

Cybercrime
Research Institute

ECONOMIC IMPORTANCE

- Extent of economic damages caused by malicious software is controversially discussed
- Statistics do not cover on economic aspects like the time private users do have to spend to protect or reinstall their systems after infection
- Many companies (esp. small and medium size businesses) do not report attacks and costs



Cybercrime
Research Institute

VIRUS

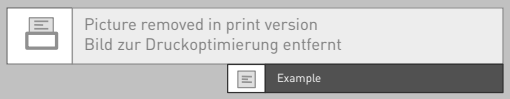
- Many similarities to biological viruses (biological virus spreads by inserting itself into living cells / Polymorphic compputer viruses have the ability to change themselves each time they replicate)
- Boot sector virus
- Companion virus
- Email virus
- Logic bomb and time bomb
- Macro viruses
- Cross-site scripting virus

A computer virus is a self-replicating computer program designed to alter the way a computer operates, without the permission of the user.

Cybercrime
Research Institute

HISTORY OF VIRUSES

- 1982 the “Elk Cloner” virus was created (by Rich Skrenta). Designed for Apple OS
- 1986 “Brain Virus” was identified. Virus was designed for MS-DOS
- 1986 the the file virus “Virdem” followed
- 1990 the first polymorph virus attack “Tequila” was started



Cybercrime
Research Institute

HOW VIRUSES REPLICATE

- Replication is an essential element of viruses
- Any location with access to executable files are the key aim for viruses
- Non-resident viruses contain a module that is identifying possible targets and then infects them
- Resident viruses are distributed by operating from the memory

Picture removed in print version
Bild zur Druckoptimierung entfernt

Example

Cybercrime
Research Institute

SPEED OF THE REPLICATION

- In the past the speed of the distribution was limited due to the distribution by physical data storage media exchange
- The popularity of the Internet increased the speed of the replication dramatically
- Increasing numbers of permanently connected computers (24/7) will further increase the speed

Picture removed in print version
Bild zur Druckoptimierung entfernt

Example

Cybercrime
Research Institute

DATA INTERFERENCE

- In the past the creation of computer viruses required a high degree of technical knowledge
- Today there are tools available that enable even users without technical background to program viruses
- Microsoft publishes information about weak point of the operating system on a regular basis

Picture removed in print version
Bild zur Druckoptimierung entfernt

Example

Cybercrime
Research Institute

SYSTEM INTERFERENCE

- Businesses are increasingly depending on the availability of network and communication services
- Example: Switch from tradition high-street shops to e-commerce businesses
- But also businesses that do not offer services online might depend on network technology („Cloud Computing“)

Picture removed in print version
Bild zur Druckoptimierung entfernt

E-COMMERCE WEBSITE

Cybercrime
Research Institute

SYSTEM INTERFERENCE

- Example: Denial-of-Service Attacks
- Definition: attempt to make a computer resource unavailable to its intended users
- Distributed DoS attack: DDoS attack occurs when multiple compromised systems flood the bandwidth of a targeted system.

Cybercrime
Research Institute

NETWORK ATTACKS

Two different ways to carry out the offence:

- Physical attacks
- Network-based attacks

Cybercrime
Research Institute

NETWORK ATTACKS

- Denial of Service (DoS) Attacks
- One of the most common attacks against computer systems and networks
- A number of free software tools can be downloaded from the internet that enable even people without special technical knowledge to create viruses and start DoS Attacks

Cybercrime
Research Institute

RESOURCES

- Critical mass is already reached
- Attacks in the context of the Wikileaks discussion highlight that a relatively small number of people can affect large businesses
- This underlines the threat level

Cybercrime
Research Institute

DEPENDANCE

- Threats of internet based attacks against critical infrastructure
- Energy, Communication, Transportation, Health, Food supply, Finance, Government services, Essential manufacturing, ...
- Even military infrastructure is depending critical technology

Picture removed in print version
Bild zur Druckoptimierung entfernt

CRITICAL INFRASTRUCTURE

Cybercrime
Research Institute

DEPENDANCE

- Alternative Communication Systems that could be used in cases of emergency are not able to cover the necessary resources
- Monoculture with regard to major technical components of computer systems, software and network technology

Picture removed in print version
Bild zur Druckoptimierung entfernt

SASSER COMPUTER WORM

Cybercrime
Research Institute

STUXNET

- Malicious software targeting Windows operating system
- Discovered in June 2010
- Specifically focussing on Supervisory Control And Data Acquisition (SCADA)
- SCADA is for example used in Siemens S7 systems that are used to control critical infrastructure such as power plants

Picture removed in print version
Bild zur Druckoptimierung entfernt

Siemens S7-300

Cybercrime
Research Institute

PAYLOAD

- Researches indicate that the software was capable of manipulating the frequency of the centrifuges at Iran's enrichment plant
- Regular speed is between 807 Hz and 1210 Hz
- The virus might have changed the frequency down to 2Hz and up to 1410Hz
- High speed and "shaking-effect" has the potential to physical damage the centrifuges

Picture removed in print version
Bild zur Druckoptimierung entfernt

APA Website

Cybercrime
Research Institute

PHYSICAL DAMAGE VIA NETWORKS

- Stuxnet underlined again that the impact of a network attacks does not need to limited to hindering data transmissions
- Various possible threat scenarios of attacks against targets that are more difficult to protect than critical infrastructure
- Recovery of hardware failure of hard drives can go along significant costs

Picture removed in print version
Bild zur Druckoptimierung entfernt

Hard Drive

Average cost of logical recover is $400 to $600, average cost of physical recovery is $1,200 - $2,000 and up to $15,000 for complex systems.

Technology News

Cybercrime
Research Institute

IMPACT

Cybercrime
Research Institute

UNCERTAINTY REGARDING EXTENT

- Lack of reporting leads to uncertainty with regard to the extent of crime
- This is especially relevant with regard to the involvement of organized crime
- Available information from the crime statistics therefore not necessary reflect the real extent of crime

The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack," explained Mark Mershon, acting head of the FBI's New York office.

HEISE NEWS 27.10.2007

Cybercrime
Research Institute

ANTI CYBERCRIME STRATEGY

Cybercrime
Research Institute

DEVELOPING COUNTRIES

- It is true that developing countries are also facing crimes that developed countries are facing
- However the priorities and capacities to prevent and investigate offences are different
- Therefore the legal solutions need to reflect these different priorities
- Developing a legal framework therefore needs to reflect two aspects: International standards and national (regional) demands

Cybercrime
Research Institute

DEVELOPING COUNTRIES

- Legal frameworks need to be adjusted to ensure that they cover the latest trends and are in line with international standards
- This is a core interest of businesses
- The current Cybercrime legislation does for example not criminalize illegal data acquisition
- It also contains investigation instruments that are significantly more intensive than international best practices

BARBADOS CMA

15. (1) Where a magistrate is satisfied, on information on oath given by a police officer, that there are reasonable grounds for suspecting that an offence under this Act has been or is about to be committed in any place and that evidence that such an offence has been or is about to be committed is in that place, the magistrate may issue a warrant authorising any police officer to enter and search that place, including any computer, using such reasonable force as is necessary.

Cybercrime
Research Institute

TRAINING

Cybercrime
Research Institute

CYBERCRIME

- Identifying storage devices can be difficult as the technology is developing so fast
- Storage devices are getting smaller and smaller and can be integrated in various tools

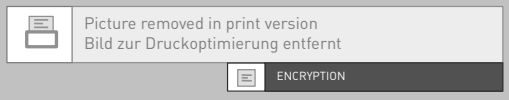
Picture removed in print version
Bild zur Druckoptimierung entfernt

PEN USB KEY

Cybercrime
Research Institute

CYBERCRIME

- Offenders that want to bring illegal material in the country do not necessary have to carry physical storage devices
- Remote storage is very popular
- Various Internet companies such as Microsoft and Google offer large server capacities for the storage of data (such as e-mail, pictures, video) that can be accessed from any place with an Internet connection



Cybercrime
Research Institute

IMPORTANCE OF E-EVIDENCE IN TRADITIONAL INVESTIGATIONS

Cybercrime
Research Institute

OPPORTUNITIES

- Case example 2: Investigator were able to discover that the suspect was searching for specific terms such as ""undetectable poisons," "fatal digoxin levels," "instant poisons," "toxic insulin levels," "how to purchase guns illegally," how to find chloroform," "fatal insulin doses," "poisoning deaths," "where to purchase guns illegally," "gun laws in PA," "how to purchase guns in PA,"

Picture removed in print version
Bild zur Druckoptimierung entfernt

PCWORLD

Cybercrime
Research Institute

DEVICES PROCESSING DATA

- Devices do often store information that are valuable for traditional investigation
- The user do not necessary have knowledge about such operation
- One example is the iPhone that stored the geo-location of the user and thereby enabled the reconstruction of movements/travel

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE: AMAZON CLOUD COMPUTING