

# “Developing a National and Organizational Cybersecurity Strategy”

**Dr David E. Probert**



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



*Committed to connecting the world*

# \* ITU Cybersecurity Strategy \*

## "3-Day Workshop Overview"

<p><b>S1- Mon: 9:30-11:00</b></p> <p>"The Cybersecurity Challenge!..."</p> <p><i>Workshop Presentations</i></p>	<p><b>S2-Mon: 11:30-13:00</b></p> <p>"The Need for Action!"</p> <p><i>Workshop Presentations</i></p>	<p><b>S3 - Mon:14:00-15:30</b> Group Session:</p> <p>"Developing the National Cybersecurity Action Plans"</p> <p><i>Group Tasks &amp; Discussions</i></p>	<p><b>S4 - Mon:16:00-17:30</b> Group Session:</p> <p>"Group Discussion: National Cybersecurity Action Plans"</p> <p><i>Group Tasks &amp; Discussions</i></p>
<p><b>S5- Tues: 9:30-11:00</b></p> <p>ITU Cyber Agenda: <b>1</b> "Cybercrime and Legislation"</p> <p><i>Workshop Presentations</i></p>	<p><b>S6-Tues: 11:30-13:00</b></p> <p>ITU Cyber Agenda: <b>2</b> "Technological Risks and Solutions"</p> <p><i>Workshop Presentations</i></p>	<p><b>S7 -Tues:14:00-15:30</b> Group Session:</p> <p>"Developing the National Legislation and Regulations"</p> <p><i>Group Tasks &amp; Discussions</i></p>	<p><b>S8 -Tues:16:00-17:30</b> Group Session:</p> <p>"Group Discussion: National Legislation and Regulations"</p> <p><i>Group Tasks &amp; Discussions</i></p>
<p><b>S9- Wed: 9:30-11:00</b></p> <p>ITU Cyber Agenda: <b>3</b> "Operational Risks and Organisational Structures"</p>	<p><b>S10-Wed:11:30-13:00</b></p> <p>ITU Cyber Agenda: <b>4&amp;5</b> "Capacity Building and Collaboration"</p>	<p><b>S11-Wed:14:00-15:30</b> Group Session:</p> <p>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</p>	<p><b>S12-Wed:16:00-17:30</b> Group Session:</p> <p>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</p>



# Securing Jamaica in Cyberspace!



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



International  
Telecommunication  
Union

Committed to connecting the world



# Jamaican & Caribbean Connectivity





# From Buccaneers to “Cyber-Pirates”!

- 17<sup>th</sup> – 19<sup>th</sup> Centuries = Maritime Security
  - Attacks & Raids from the Sea
  - Protection of Coastal Regions
  - Regional Buccaneers & Pirates
- 20<sup>th</sup> Century = Territorial & Aerial Security
  - Physical, Financial & Political Crimes
  - Networked Physical Security
  - Establishment of United Nations
- 21<sup>st</sup> Century = Global Cyber Security
  - Cybercrime, Cyber Risks & Threats
  - Emergence of Information Security
  - Establishment of the UN/ITU – GCA
    - \* Global Cybersecurity Agenda \*



# ITU: High-Level Expert Group – Global Cybersecurity Agenda

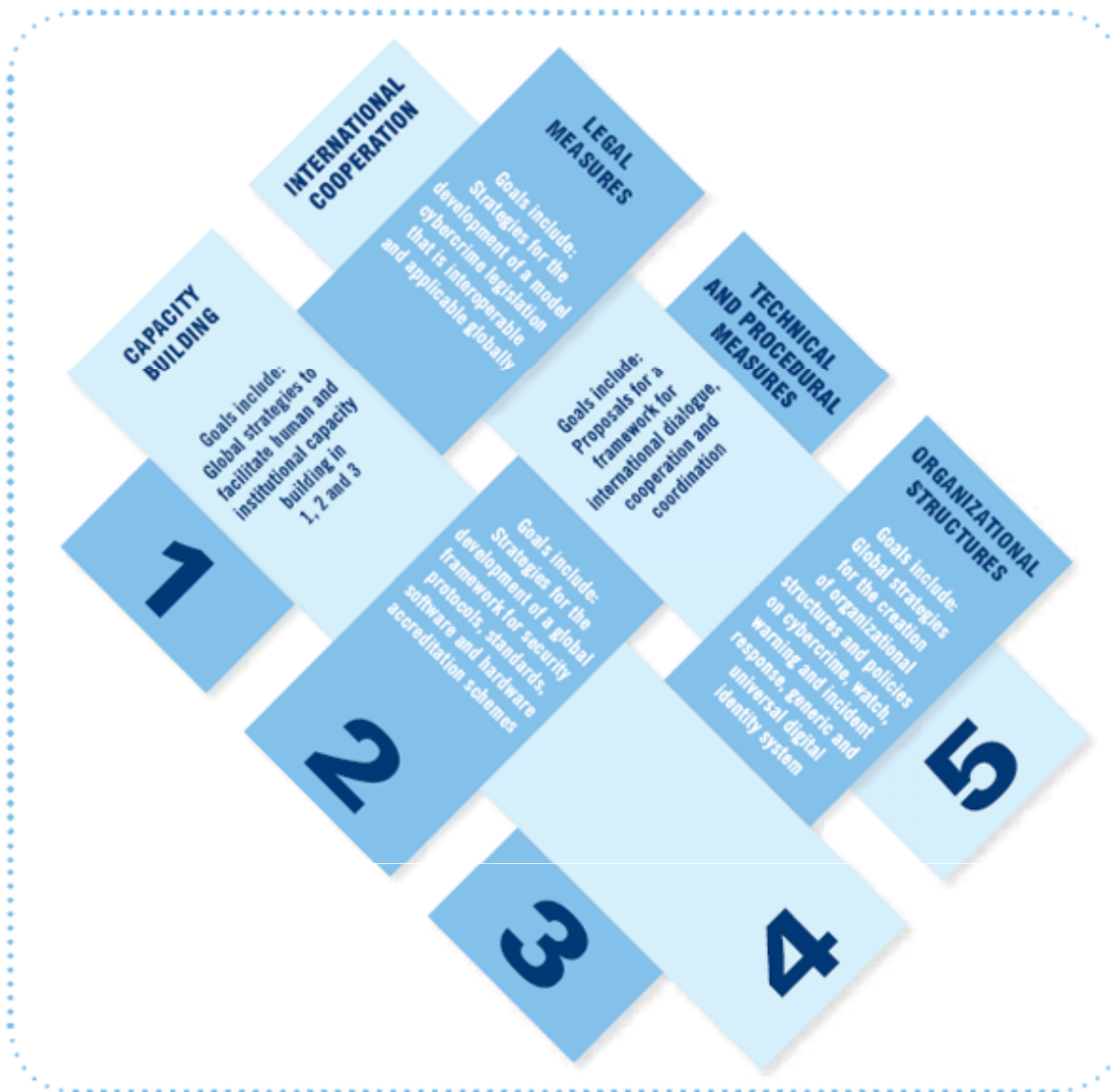


University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world



## The ITU GCA - Global Cybersecurity Agenda:

- 1 – Legal Measures
- 2 – Technical Measures
- 3 – Organisational Measures
- 4 – Capacity Building
- 5 – International Cooperation



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world



# ITU GCA – Seven Strategic Goals

## The Seven Goals:

- 1 Elaboration of strategies for the development of a **model cybercrime legislation** that is globally applicable and interoperable with existing national and regional legislative measures.
- 2 Elaboration of global strategies for the creation of appropriate national and regional **organizational structures** and policies on **cybercrime**.
- 3 Development of a strategy for the establishment of globally accepted minimum **security criteria and accreditation schemes for hardware and software applications and systems**.
- 4 Development of strategies for the creation of a global framework for **watch, warning and incident response** to ensure cross-border coordination between new and existing initiatives.
- 5 Development of global strategies for the creation and endorsement of a **generic and universal digital identity system** and the necessary **organizational structures** to ensure the recognition of digital credentials across geographical boundaries.
- 6 Development of a *global strategy to facilitate* **human and institutional capacity building** to enhance knowledge and know-how across sectors and in all the above-mentioned areas.
- 7 Proposals on a framework for a *global multi-stakeholder strategy* for **international cooperation, dialogue and coordination** in all the above-mentioned areas.

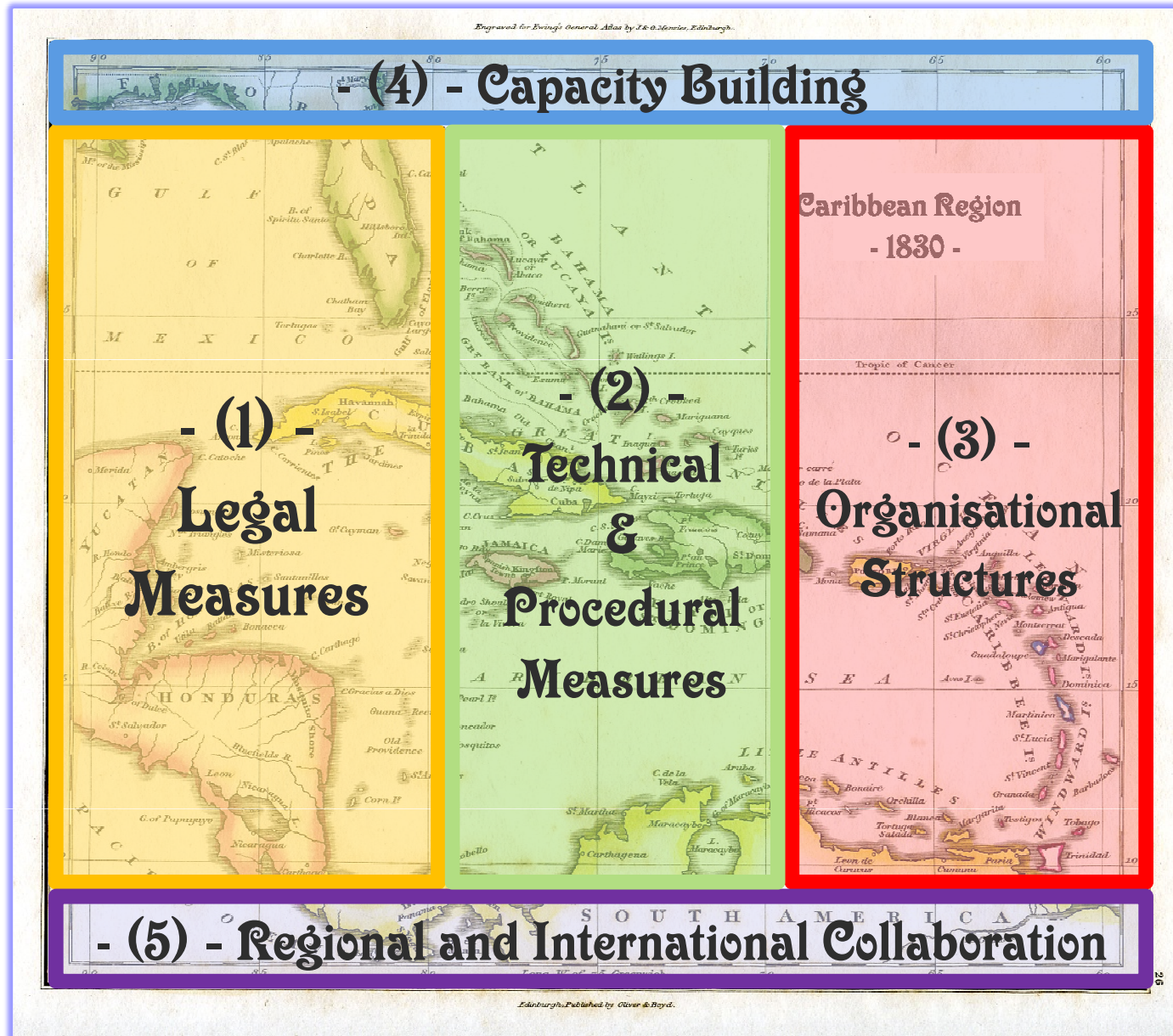


# Securing Jamaica in Cyberspace!

## - (4) - Capacity Building



# Securing the Caribbean in Cyberspace!





# \* ITU Cybersecurity Strategy \*

## *"3-Day Workshop Overview"*

<b>S1- Mon: 9:30-11:00</b>  <b>"The Cybersecurity Challenge!..."</b>	<b>S2-Mon: 11:30-13:00</b>  <b>"The Need for Action!"</b>	<b>S3 - Mon:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Cybersecurity Action Plans"</b>	<b>S4 - Mon:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Cybersecurity Action Plans"</b>
<b>S5- Tues: 9:30-11:00</b>  <b>ITU Cyber Agenda: 1</b> <b>"Cybercrime and Legislation"</b>	<b>S6-Tues: 11:30-13:00</b>  <b>ITU Cyber Agenda: 2</b> <b>"Technological Risks and Solutions"</b>	<b>S7 -Tues:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Legislation and Regulations"</b>	<b>S8 -Tues:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Legislation and Regulations"</b>
<b>S9- Wed: 9:30-11:00</b>  <b>ITU Cyber Agenda: 3</b> <b>"Operational Risks and Organisational Structures"</b>	<b>S10-Wed:11:30-13:00</b>  <b>ITU Cyber Agenda: 4&amp;5</b> <b>"Capacity Building and Collaboration"</b>	<b>S11-Wed:14:00-15:30</b> <b>Group Session:</b>  <b>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</b>	<b>S12-Wed:16:00-17:30</b> <b>Group Session:</b>  <b>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</b>



# \* Workshop Session 1 \*

## The Cybersecurity Challenge

<b>1 – Jamaica in Cyberspace</b>	<b>2 - Stakeholders</b>	<b>3 – Critical Service Sectors</b>
<b>4 – Cyber Threats</b>	<b>5 – Cyber Attacks</b>	<b>6 – Recent Case Studies</b>
<b>7 - \$\$\$ Financial Impacts</b>	<b>8 – Trade &amp; Political Impacts</b>	<b>9 - Jamaica: Strategic Needs</b>



# \* Workshop Session 1 \*

## The Cybersecurity Challenge

<b>1 – Jamaica in Cyberspace</b>	<b>2 - Stakeholders</b>	<b>3 – Critical Service Sectors</b>
<b>4 – Cyber Threats</b>	<b>5 – Cyber Attacks</b>	<b>6 – Recent Case Studies</b>
<b>7 - \$\$\$ Financial Impacts</b>	<b>8 – Trade &amp; Political Impacts</b>	<b>9 - Jamaica: Strategic Needs</b>





# “Securing Jamaica in Cyberspace”

- During this 3-day intensive ITU Workshop we’ll work together to develop:
  - An Action Plan for Cybersecurity in Jamaica
  - Models for National & Organizational Cybersecurity Agencies
  - An Outline Action Roadmap for Implementing and Managing Cybersecurity within Jamaica during the next 12 – 18 months
- We begin by exploring the threats from cybercrime & cyber attacks upon the government & business sectors.



# **\* Workshop Session 1 \***

## **The Cybersecurity Challenge**

<b>1 – Jamaica in Cyberspace</b>	<b>2 - Stakeholders</b>	<b>3 – Critical Service Sectors</b>
<b>4 – Cyber Threats</b>	<b>5 – Cyber Attacks</b>	<b>6 – Recent Case Studies</b>
<b>7 - \$\$\$ Financial Impacts</b>	<b>8 – Trade &amp; Political Impacts</b>	<b>9 - Jamaica: Strategic Needs</b>



# Cybersecurity Stakeholders

- Everyone sector has some interest in cybersecurity:
  - *Jamaican Government*: Ministries, Parliament, Regional & Local Administrations, Military & Civil Defence, Emergency Services
  - *Jamaican Business Sectors*: Banking, Financial, Airline, Road & Rail Transportation, Telecommunications, Power & Water Utilities, Education, Healthcare, Tourism, Agriculture & Manufacturing.
  - *Jamaican Citizens*: Risk of Personal Identify Theft and Losses from On-Line Cybercrimes such as Phishing Attacks, Spam, & Hacking.





# **\* Workshop Session 1 \***

## **The Cybersecurity Challenge**

<b>1 – Jamaica in Cyberspace</b>	<b>2 - Stakeholders</b>	<b>3 – Critical Service Sectors</b>
<b>4 – Cyber Threats</b>	<b>5 – Cyber Attacks</b>	<b>6 – Recent Case Studies</b>
<b>7 - \$\$\$ Financial Impacts</b>	<b>8 – Trade &amp; Political Impacts</b>	<b>9 - Jamaica: Strategic Needs</b>



# Critical Service Sectors (Business)

- Every nation is dependant upon critical service sectors in order to function efficiently for its citizens...  
....These are the sectors that may be the targets for cyberattacks from criminals, terrorists or hackers.
  - Critical Sectors within the Jamaican Economy would certainly include:
    - Travel, Transportation and Tourism
    - Banking and Financial Institutions
    - Power and Water Utilities Network
    - Telecommunications and Mobile Networks
    - Agriculture & Fisheries Production Value-Chain
- .....*Cybersecurity is not just a technological ICT issue!*



# Critical Service Sectors (Government)

- Overall responsibility for cybersecurity strategy, laws and regulations lies with the Jamaican Government & Cabinet Ministries including:
  - *Office of the Prime Minister* – Overall responsibility for national cybersecurity strategy, organisation and implementation.
  - *Ministry of National Security* – Specific in-depth responsibility for the management & integration of cybersecurity within the fields of physical, information, intelligence & communications security.
  - *Ministry of Justice* – Developing of Legislation & Regulations against the threats from cybercrimes & cyberattacks
  - *Ministry of Finance* – Protection of the national banking & financial services infrastructure in partnership with banking sector.
  - *Ministry of Foreign Affairs* – Collaboration with international partners to combat cybercrime, cyber attacks & cyber terrorism.



# Cybersecurity for US Defence: “The Pentagon’s Cyberstrategy”



The screenshot shows the homepage of the Foreign Affairs magazine website. At the top, the logo for Foreign Affairs is displayed, featuring a circular emblem with a horse and rider, and the text 'FOREIGN AFFAIRS' in a serif font. Below the logo, it says 'Published by the Council on Foreign Relations'. To the right of the logo, there are links for 'Home', 'International Editions', and 'Newsstand Finder'. Below the logo, there is a navigation bar with links for 'About Us', 'In the Magazine', 'Regions', 'Topics', 'Features' (highlighted in red), 'Discussions', and 'Books & Reviews'. Below the navigation bar, there is a breadcrumb trail: 'Home > Features > Essays > Defending a New Domain'. The main title of the article is 'Defending a New Domain' in a large, bold, black font. Below the title, the subtitle is 'The Pentagon's Cyberstrategy'. The author is 'By William J. Lynn III' in red text. The date is 'September/October 2010'. Below the article information, there is a row of social media sharing icons: 'PRINT', 'EMAIL', 'SHARE', 'TEXT', and a plus sign. Below the sharing icons, there is a 'Summary' section with the text: 'Right now, more than 100 foreign intelligence organizations are trying to hack into the digital networks that undergird U.S. military operations. The Pentagon recognizes the catastrophic threat posed by cyberwarfare, and is partnering with allied governments and private companies to prepare itself.' Below the summary, there is a bio for William J. Lynn III: 'WILLIAM J. LYNN III is U.S. Deputy Secretary of Defense.'



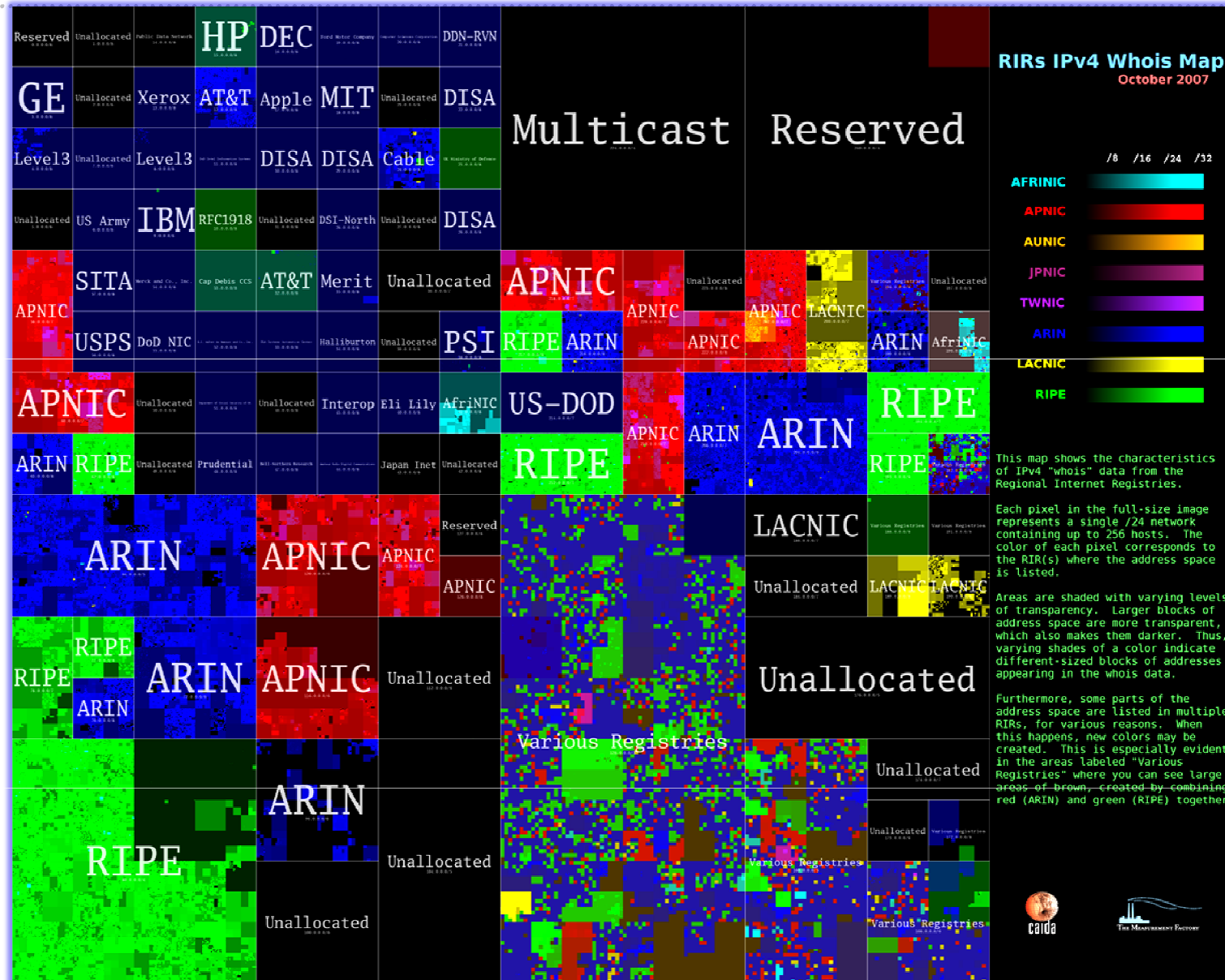
# \* Workshop Session 1 \*

## The Cybersecurity Challenge

1 – Jamaica in Cyberspace	2 - Stakeholders	3 – Critical Service Sectors
4 – Cyber Threats	5 – Cyber Attacks	6 – Recent Case Studies
7 - \$\$\$ Financial Impacts	8 – Trade & Political Impacts	9 - Jamaica: Strategic Needs



# "Visualisation of Cyberspace": Global IP WHOIS Addresses



# Cyber Threats

- *Cyber Criminals*: Digital Fraud & Forgery, Extortion, Digital “Advanced Fee” Scams, ID Theft, Digital Money Laundering, Offensive & Pornographic Materials, Drug Trafficking, Cyber Stalking & Hate Crimes.
- *Cyber Terrorists*: Denial of Service, Website Defacement, Theft of Secret Information & Intelligence, On-Line Blackmail, Disruption of Critical Infrastructure such as Airports, Power Stations, Hospitals, and the National Clearing Banking Networks.
- *Cyber Warfare*: Closely related to cyber terrorism, and applied when there is a concerted cyber attack from a region or nation against the infrastructure and citizens of some other defined region or nation.
- *Cyber Hackers*: Skilled Individuals and “Researchers” that will initiate malicious attacks for the penetration of secure systems and theft of secret documents & databases from both governments & businesses.

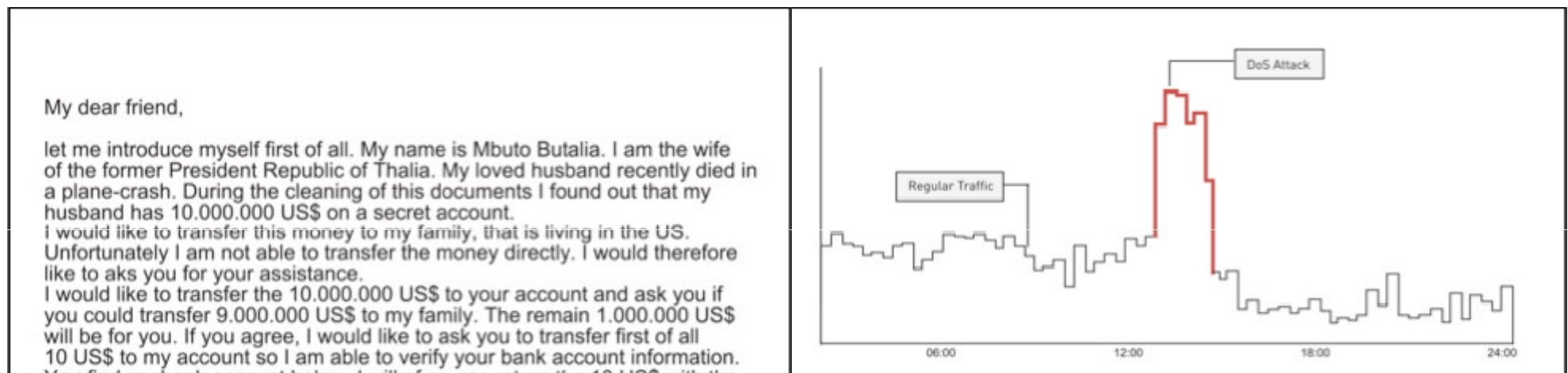


# Typical Cybercrime Threats



(a) – Hardware & Software Keyloggers

(b) – Email Phishing



(c) – Advance Fee Scam

(d) – Denial of Service



# Cybercrime in Jamaica

## Cyber security alert - Government, private sector meet to safeguard cyber knowledge

published: Thursday | March 18, 2004

By Leonardo Blair, Staff Reporter



POINTING TO the recent loss of millions of dollars by RBTT Bank Jamaica Ltd. through its automated teller system, Dr. Peter Phillips, Minister of National Security, yesterday said the Government was now paying increased attention to incidents of cyber crimes.

## Cyber crime investigation bears fruit

Published: Thursday | August 27, 2009



**A two-year cyber crime investigation by the Organised Crime Investigation Division (OCID) has led to the arrest of a 26-year-old computer specialist in upper St Andrew on the weekend and three others yesterday.**



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world

# Jamaican Cybercrime & Counterfeiting : 2010

## Cybercrime, cigarette counterfeiting ring members held

Two of three men said to be involved in a cybercrime and cigarette counterfeiting ring were held yesterday by members of the Organised Crime Investigation Division (OCID) following a major [operation](#) at Shenstone Drive in Beverly Hills, St Andrew.

According to the police, several boxes of cigarettes of different brands, cash in local and foreign currencies and boxes of expensive liquor was seized during the operation.

seized money

"Investigations into the matter are being carried out but we cannot just yet say how much money was seized," head of the OCID Superintendent Fitz Bailey said.

He, however, said that the seized money which included Canadian dollars and [pound](#) sterling could amount to several million dollars.

The three men who were found at the house were held and are to be questioned.

*The Jamaica Online*  
**STAR**



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world

# Jamaica: Lottery Scam

## Eight persons arrested during massive operation by OCID

March 14, 2009 – 8:31 pm



Eight persons including one of the major players in the lottery scam and a Police Constable were arrested in St James yesterday during a massive operation by members of the Organized Crime Investigative Division (OCID).

Reports from the Constabulary Communication Network are that between 5:00 a.m. and 1:30 p.m. yesterday, members of the Organized Crime Investigative Division, the Area One Police and the Mobile Reserve executed an operation in several communities in St. James. During the exercise, eight persons; three women and five men, including one of the main players in the illegal lottery operation, a Police Constable who is on interdiction and two brothers who had absconded bail on previous charges were apprehended. The eight are to be interviewed soon by senior investigators from OCID.



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world

# USB Memory Stick: Cybersecurity Info Risk

## USB stick containing police information on riot control and officers' names and ranks found on a pavement

Dan Raywood September 06, 2010



PRINT



EMAIL



REPRINT

FONT SIZE: A|A|A

BOOKMARK



A lost USB stick that contained police information described as 'dynamite' was found in the street outside a station.

According to [reports](#), a stick containing more than 2,000 pages of highly sensitive and confidential information, intended to be seen only by senior officers, was found on a pavement near a Greater Manchester police station.

The USB stick was prominently branded with the Greater Manchester Police logo and included detailed strategies for acid and petrol bomb attacks, blast control training and the use of batons and shields. It also had a comprehensive list of officers' names, ranks and their divisions.

### RELATED ARTICLES

- Information Commissioner's Office finds three county councils in breach of the Data Protection Act after losing data on children



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica

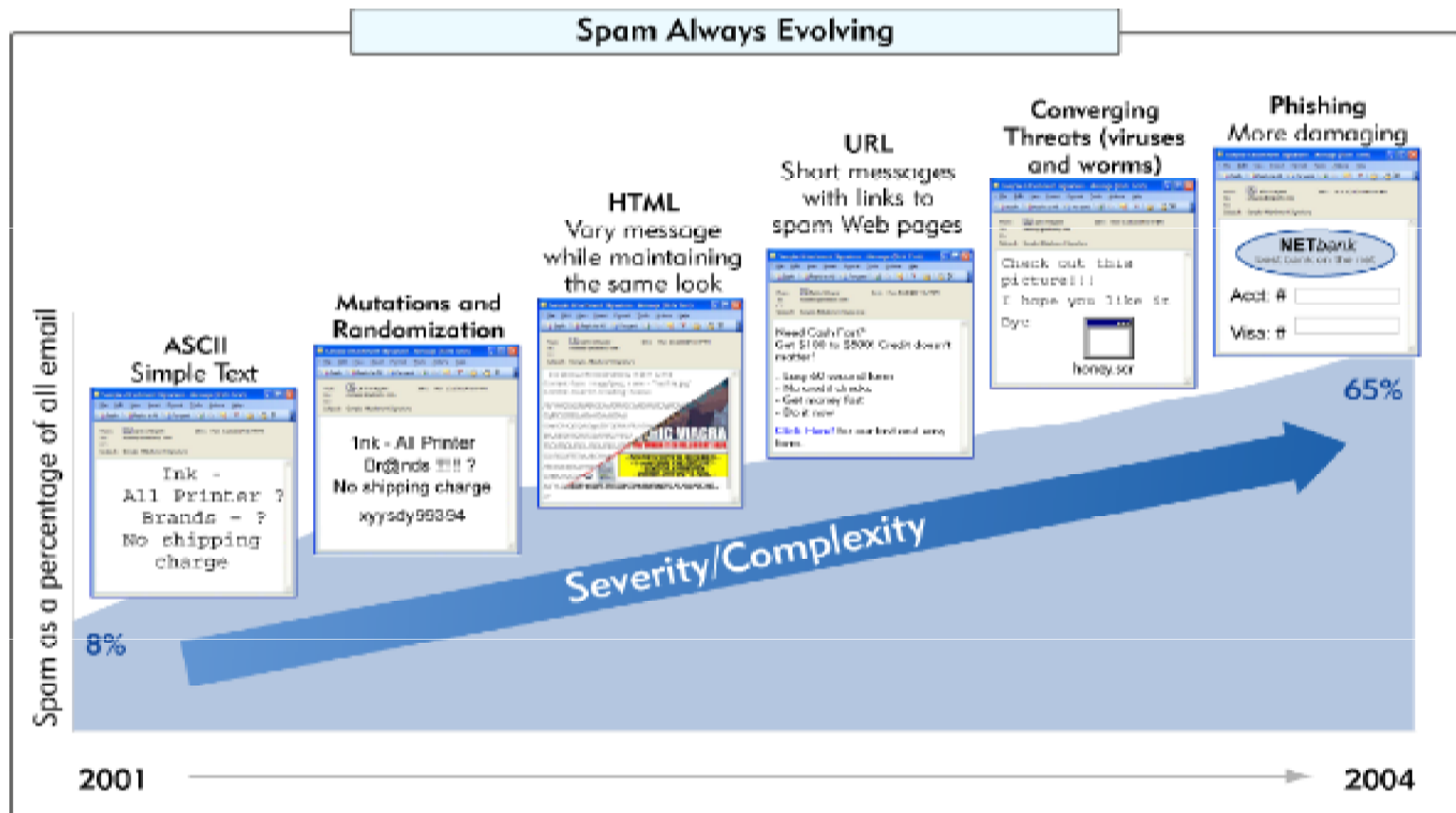


International  
Telecommunication  
Union

Committed to connecting the world



# Evolution of Spam Attacks



# Typical “Botnet” Cyberattack



# **\* Workshop Session 1 \***

## **The Cybersecurity Challenge**

<b>1 – Jamaica in Cyberspace</b>	<b>2 - Stakeholders</b>	<b>3 – Critical Service Sectors</b>
<b>4 – Cyber Threats</b>	<b>5 – Cyber Attacks</b>	<b>6 – Recent Case Studies</b>
<b>7 - \$\$\$ Financial Impacts</b>	<b>8 – Trade &amp; Political Impacts</b>	<b>9 - Jamaica: Strategic Needs</b>



# Cyber Attacks

- Industrialisation and Mainstreaming of Cyber Attacks:
  - *(1) Researchers & Cyber Software Creators of Malicious Codes* : Often creative talented computer scientists that have turned their skills to tools for illegal penetration & control of secure systems
  - *(2) "Botnet" - Farmers & Herders* : They are responsible for the illegal international distribution and infection of target "zombie" networked laptops PCs & Servers within homes and offices. The malicious codes (malware such as viruses & trojans) are spread through spam emails, infected websites and "backdoor" attacks.
  - *(3) "Commercial Botnet Dealers"* : They sell access to herds of "zombie" infected machines. The embedded malicious code can be triggered to stimulate "Denial of Service (DDoS)" attacks on target servers & websites. The aim is usually to maximise economic and political damage upon the targeted nation and associated businesses.

.....For further information see the ITU "BotNet" Mitigation Toolkit(2008)



# \* Workshop Session 1 \*

## The Cybersecurity Challenge

1 – Jamaica in Cyberspace	2 - Stakeholders	3 – Critical Service Sectors
4 – Cyber Threats	5 – Cyber Attacks	6 – Recent Case Studies
7 - \$\$\$ Financial Impacts	8 – Trade & Political Impacts	9 - Jamaica: Strategic Needs





# Recent Cyber Case Studies

- *Estonia : May 2007*
  - Targeted at Government & Banking Servers – and immobilised national & commercial economic infrastructure for several days
- *Georgia : August 2008*
  - Targeted at Government Servers including Parliament & Ministry of Foreign Affairs, and the National & Commercial Banking Network.
- *South Korea : July 2009*
  - Targets included the Defence Ministry, Presidential Offices, National Assembly, and Korea Exchange Banks. This attack was also simultaneously targeted at various high-profile US Sites & Servers such as the NY Stock Exchange, White House & Pentagon.

.....*Small scale penetrations & cyber attacks continue on an almost 24/7 against certain countries, targeted regimes and business interests.*



# \* Workshop Session 1 \*

## The Cybersecurity Challenge

1 – Jamaica in Cyberspace	2 - Stakeholders	3 – Critical Service Sectors
4 – Cyber Threats	5 – Cyber Attacks	6 – Recent Case Studies
7 - \$\$\$ Financial Impacts	8 – Trade & Political Impacts	9 - Jamaica: Strategic Needs



# \$\$\$ Financial Impacts

- Cyber attacks can have significant financial & commercial impacts including:
  - **Banks:** Partial Loss of Banking & Financial Revenues during period of attacks on banking infrastructure such as the national clearing bank & retail ATM networks. There may also be loss of bank account and credit card details which will compromise customers.
  - **Airports:** Possible closure of national airline transportation hubs such as International (Kingston) and Regional Airports (Montego Bay), which in turn will result in lost tourist, hotel and resort revenues.
  - **Investment:** Following cyber attacks there may be some of confidence in the targeted nation with regards to the resilience of its critical service infrastructure. This will in turn result in reduced foreign investment, fewer tourists and reduced business growth.



# \$ IMPACT: Trade, Economics and Public Finance

Sub-category	Impact Level 0	Impact Level 1	Impact Level 2	Impact Level 3	Impact Level 4	Impact Level 5	Impact Level 6
<b>Impact on Public Finances</b>	Minimal impact	Cause a loss to Public Sector of up to £10,000	Cause a loss to Public Sector of up to £1 million	Cause a loss to HMG/Public Sector of £millions	Cause a loss to HMG/ Public Sector of £10s millions	Cause short term material damage to national finances or economic interests (to an estimated total up to £1 billion)	Cause major, long term damage to the economy (to an estimated total in excess of £10s billions)
<b>Impact on Trade and Commerce</b>	None	None	Undermine the financial viability of a number of UK SMEs	Undermine the financial viability of a minor UK-based or UK-owned organisation	Undermine the financial viability of a major UK-based or UK-owned organisation	Cause material damage to international trade or commerce, directly and noticeably reducing economic growth in the UK	Cause major, long term damage to global trade or commerce, leading to prolonged recession or hyperinflation in the UK



# \* Workshop Session 1 \*

## The Cybersecurity Challenge

1 – Jamaica in Cyberspace	2 - Stakeholders	3 – Critical Service Sectors
4 – Cyber Threats	5 – Cyber Attacks	6 – Recent Case Studies
7 - \$\$\$ Financial Impacts	8 – Trade & Political Impacts	9 - Jamaica: Strategic Needs





# Trade & Political Impacts

- Besides the financial impacts, cyberattacks could have wider impacts upon Jamaica including:
  - **Confidence:** Loss of confidence in the government's ability to defend the nation, critical service infrastructure and the economy in cyberspace
  - **Tourism:** Significant reduction in travel, tourism and resort revenues
  - **Trade:** Temporary closure of the Banking & Financial Infrastructure following major cyber attacks could lead to suspension of trade & exports of high value agricultural produce within Jamaican Ports
  - **Defence:** Possible Loss of secret government, military and defence data & information, maybe through stolen laptops, memory chips, or penetrated "secure" servers by malicious code of compromised staff



# \* Workshop Session 1 \*

## The Cybersecurity Challenge

1 – Jamaica in Cyberspace	2 - Stakeholders	3 – Critical Service Sectors
4 – Cyber Threats	5 – Cyber Attacks	6 – Recent Case Studies
7 - \$\$\$ Financial Impacts	8 – Trade & Political Impacts	9 - Jamaica: Strategic Needs



# Jamaica: Strategic Cyber Agenda

- Jamaica's Security in 21stC Cyberspace requires:
  - (1) – Upgraded Laws, Legislation, Polices and Regulations
  - (2) – New Technological Measures and Operational Procedures
  - (3) - National Jamaican Government Cybersecurity Agency
  - (4) - Cybersecurity Teams within major businesses and critical service sectors such as Banking/Finance, Energy & Water Utilities, Telecommunications, Transportation, Ports, Tourism, & Agriculture
  - (5) - Cybersecurity Cultural Awareness and Professional Training Courses leading to Certification to accepted International Standards
  - (6) - International Collaboration and Partnerships with organisations such as Interpol that are focused upon tackling global cybercrime.



# \* ITU Cybersecurity Strategy \*

## "3-Day Workshop Overview"

<b>S1- Mon: 9:30-11:00</b>  <b>"The Cybersecurity Challenge!..."</b>	<b>S2-Mon: 11:30-13:00</b>  <b>"The Need for Action!"</b>	<b>S3 - Mon:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Cybersecurity Action Plans"</b>	<b>S4 - Mon:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Cybersecurity Action Plans"</b>
<b>S5- Tues: 9:30-11:00</b>  <b>ITU Cyber Agenda: 1</b> <b>"Cybercrime and Legislation"</b>	<b>S6-Tues: 11:30-13:00</b>  <b>ITU Cyber Agenda: 2</b> <b>"Technological Risks and Solutions"</b>	<b>S7 -Tues:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Legislation and Regulations"</b>	<b>S8 -Tues:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Legislation and Regulations"</b>
<b>S9- Wed: 9:30-11:00</b>  <b>ITU Cyber Agenda: 3</b> <b>"Operational Risks and Organisational Structures"</b>	<b>S10-Wed:11:30-13:00</b>  <b>ITU Cyber Agenda: 4&amp;5</b> <b>"Capacity Building and Collaboration"</b>	<b>S11-Wed:14:00-15:30</b> <b>Group Session:</b>  <b>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</b>	<b>S12-Wed:16:00-17:30</b> <b>Group Session:</b>  <b>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</b>



# \* Workshop Session 2 \*

## The Need for Action!

<b>1 – Aim: Jamaican Action Plan</b>	<b>2 – Cybersecurity Costs</b>	<b>3 – Annual Cyber-Budgets</b>
<b>4 – Cybersecurity Benefits</b>	<b>5 – Benefits: Critical Sectors</b>	<b>6 – National Case Studies</b>
<b>7 – Jamaican Cyber Strategy</b>	<b>8 – ITU GCA Strategic Pillars</b>	<b>9 – Organisational RoadMap</b>





# \* Workshop Session 2 \*

## The Need for Action!

<b>1 – Aim: Jamaican Action Plan</b>	<b>2 – Cybersecurity Costs</b>	<b>3 – Annual Cyber-Budgets</b>
<b>4 – Cybersecurity Benefits</b>	<b>5 – Benefits: Critical Sectors</b>	<b>6 – National Case Studies</b>
<b>7 – Jamaican Cyber Strategy</b>	<b>8 – ITU GCA Strategic Pillars</b>	<b>9 – Organisational RoadMap</b>

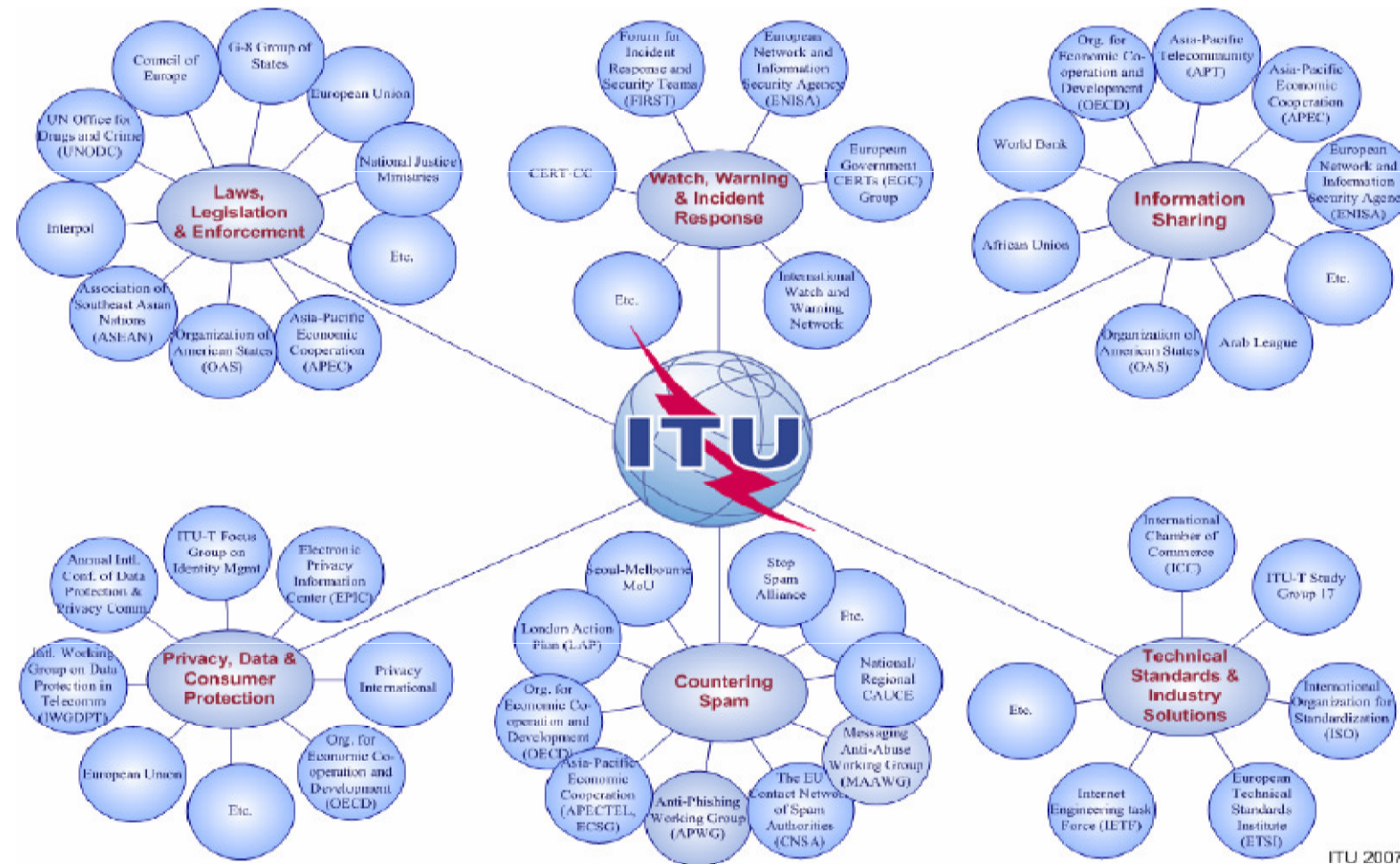


# Towards the Jamaican Action Plan

- *Action Plan:* During this session we outline the essential features of a Cybersecurity Action Plan for Jamaica
- *Cost Benefits Analysis:* We'll also consider the Economic Case for Action based upon a "Cost Benefit Analysis" and the multi-year "Total Cost of Ownership" (TCO) for the Jamaican government & major businesses
- *National Case Studies:* There are already numerous models for national cybersecurity actions plans from countries in Europe, the Americas, Asia and the Far East



# International Stakeholders for the Cybersecurity Ecosystem



ITU 2007



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



International  
Telecommunication  
Union

Committed to connecting the world

# \* Workshop Session 2 \*

## The Need for Action!

1 – Aim: Jamaican Action Plan	2 – Cybersecurity Costs	3 – Annual Cyber-Budgets
4 – Cybersecurity Benefits	5 – Benefits: Critical Sectors	6 – National Case Studies
7 – Jamaican Cyber Strategy	8 – ITU GCA Strategic Pillars	9 – Organisational RoadMap



# Cybersecurity Costs : Short-Term

- 1) *National Cyber Agency*: Establishment of a possible National Jamaican Cybersecurity Agency within the Central Government Ministries
- 2) *CIIP*: Long Term Critical Information Infrastructure Protection (CIIP)
- 3) *System Upgrades*: Technical Infrastructure Upgrades including Hardware, Software, Databases, Secure Network Links, Biometrics & RFID
- 4) *Back-Up*: Disaster Recovery, Business Continuity and Back-Up Systems
- 5) *Physical* : Physical Security Applications – CCTV, Alarms, Control Centre
- 6) *Awareness Campaign*: Government Campaign for cybersecurity awareness
- 7) *Training*: National Cybersecurity Skills & Professional Training Programme
- 8) *Encryption*: National User & Systems PKI Authentication Programme
- 9) *Laws*: Costs for Drafting and Enforcing Cyber Laws. Policies & Regulations





# \* Workshop Session 2 \*

## The Need for Action!

1 – Aim: Jamaican Action Plan	2 – Cybersecurity Costs	3 – Annual Cyber-Budgets
4 – Cybersecurity Benefits	5 – Benefits: Critical Sectors	6 – National Case Studies
7 – Jamaican Cyber Strategy	8 – ITU GCA Strategic Pillars	9 – Organisational RoadMap



# Annual Cybersecurity Budgets

- Managing cybersecurity is an ongoing task with a continuous need for government & business systems upgrades, staff training, and response to emergency cyber events & alerts
- Annual Security Budgets will need to include allowances for:
  - Staff salaries & operational costs for the proposed National Cyber Agency
  - Costs for tackling cybercrime through a possible National Cybercrime Unit
  - Management of cybersecurity by Jamaican Military & Defence Organisation
  - Costs of required annual security audits to ensure ongoing compliance
  - Professional training courses at leading Jamaican Institutions such as UTECH
  - Costs for maintaining “best practice” cybersecurity within each of the critical service sectors within the Jamaican Economy such as Banking, Tourism & Trade
  - Regular Systems, Computing & Communications reviews & upgrades for all secure government computing centres, as well as those for major enterprises
  - On-going costs to support extensive international partnerships & collaboration



# \* Workshop Session 2 \*

## The Need for Action!

1 – Aim: Jamaican Action Plan	2 – Cybersecurity Costs	3 – Annual Cyber-Budgets
4 – Cybersecurity Benefits	5 – Benefits: Critical Sectors	6 – National Case Studies
7 – Jamaican Cyber Strategy	8 – ITU GCA Strategic Pillars	9 – Organisational RoadMap



# Cybersecurity Benefits: Government

- Improved cybersecurity provides significant benefits to the Government & Critical National Utilities including:
  - **eGovernment:** Fully secure & cost effective delivery of on-line services to both citizens and businesses, such as taxes & customs, social welfare, civil & land registries, passports & driving licences
  - **eDefence:** Early warning, alerts and defences against cyberattacks through national CERT (Computer Emergency Response Centre)
  - **Cybercrime:** Investigate, Digital Forensics and Prosecution of cybercrimes such ID & Financial Theft, "Computer Misuse, Laundering, On-Line Drug Trafficking & Pornographic Materials
  - **Cyberterrorism:** Ability to assess, predict and prevent potential major cyber terrorist attacks, and to minimise damage during events
  - **Power & Water Utilities:** Prevent malicious damage to control systems
  - **Telecommunications:** Top security of government communications with alternative routings, encryption & protection against cyberattack



# **\* Workshop Session 2 \***

## **The Need for Action!**

<b>1 – Aim: Jamaican Action Plan</b>	<b>2 – Cybersecurity Costs</b>	<b>3 – Annual Cyber-Budgets</b>
<b>4 – Cybersecurity Benefits</b>	<b>5 – Benefits: Critical Sectors</b>	<b>6 – National Case Studies</b>
<b>7 – Jamaican Cyber Strategy</b>	<b>8 – ITU GCA Strategic Pillars</b>	<b>9 – Organisational RoadMap</b>





# Business Benefits: Critical Sectors

- **Banking & Finance:** This sector, at the heart of the economy, has most to gain from improved cybersecurity for its financial databases, secure transactions & national networks
- **Air Transportation:** Island Jamaica is totally dependant upon the security and safety of its airport infrastructure including the facilities, airline networks, staff, assets & support services
- **Travel & Tourism:** International visitors and tourists place a high value upon personal safety & security, so improved cybersecurity & reduced cybercrime will help boost tourism revenues
- **Agriculture & Fisheries:** Even the Jamaican agricultural value-chain has a high dependence upon secure computing applications & networks
- **Ports & International Trade:** International trade is now highly automated with real-time management of the Jamaican Ports & Export/Import Shipments. Cybersecurity upgrades will improve the overall security, and system resilience to malicious attacks by criminals or terrorists.



# \* Workshop Session 2 \*

## The Need for Action!

1 – Aim: Jamaican Action Plan	2 – Cybersecurity Costs	3 – Annual Cyber-Budgets
4 – Cybersecurity Benefits	5 – Benefits: Critical Sectors	6 – National Case Studies
7 – Jamaican Cyber Strategy	8 – ITU GCA Strategic Pillars	9 – Organisational RoadMap



# National Security Case Studies

- **UK Government:** Cybersecurity Strategy for the UK – Safety, Security & Resilience in Cyberspace (UK Office of Cybersecurity – June 2009)
- **US Government:** Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure – May 2009
- **Canada:** Canadian Cyber Incident Response Centre (CCIRC) – Integrated within the Strategic Government Operations Centre (GOC)
- **Australia:** Australian Cybersecurity Policy and Co-ordination Committee (CSPC – Nov 2009), within the Attorney-General's Government Dept
- **Malaysia:** "Cybersecurity Malaysia" – Mosti : Ministry of Science, Technology & Innovation, and includes the MyCERT & Training Centre
- **Singapore:** Cybersecurity Awareness Alliance & the IDA Security Masterplan (Sept 2009) -Singapore Infocomm Technology Security Authority - SITSA
- **South Korea:** Korea Internet and Security Agency (KISA – July 2009)
- **Latin America :** CITEC/OAS has developed regional cybersecurity strategy
- **European Union:** ENISA – European Network and Information Security Agency (September 2005) tackles all aspects of cybersecurity & cybercrime for the countries of the European Union and beyond



# UK Office of Cybersecurity – OCS & CSOC



## Cyber Security Strategy of the United Kingdom

safety, security and resilience in cyber space



To address the UK's cyber security challenges, the Government will:

- **Establish a cross-government programme**, with additional funding to address the following priority areas in pursuit of the UK's strategic cyber security objectives:
  - Safe Secure & Resilient Systems
  - Policy, Doctrine, Legal & Regulatory issues
  - Awareness & Culture Change
  - Skills & Education
  - Technical Capabilities & Research and Development
  - Exploitation
  - International Engagement
  - Governance, Roles & Responsibilities
- **Work closely with** the wider public sector, industry, civil liberties groups, the public and with international **partners**;
- **Set up an Office of Cyber Security (OCS)** to provide strategic leadership for and coherence across Government;
- **Create a Cyber Security Operations Centre (CSOC)** to:
  - actively monitor the health of cyber space and co-ordinate incident response;
  - enable better understanding of attacks against UK networks and users;
  - provide better advice and information about the risk to business and the public.



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world

# US Government : Cybersecurity Review

**TABLE 1: NEAR-TERM ACTION PLAN**

1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics.
4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5. Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.
6. Initiate a national public awareness and education campaign to promote cybersecurity.
7. Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
8. Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement
9. In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
10. Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

**\* 60-Day \*  
Policy Review**



**May 2009**

**TABLE 3: MID-TERM ACTION PLAN**

1. Improve the process for resolution of interagency disagreements regarding interpretations of law and application of policy and authorities for cyber operations.
2. Use the OMB program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity goals.
3. Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.
4. Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government.
5. Determine the most efficient and effective mechanism to obtain strategic warning, maintain situational awareness, and inform incident response capabilities.
6. Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of R&D.
7. Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.
8. Develop mechanisms for cybersecurity-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.
9. Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality.
10. Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.
11. Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.
12. Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies.
13. Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.
14. Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services.



University of Technology,  
Jamaica

**ITU Centres of Excellence Network for the Caribbean Region**  
**Developing a National and Organizational Cybersecurity Strategy**  
*13-15 September, Kingston, Jamaica*



**Committed to connecting the world**



# Canadian Government

- The Canadian Cyber Incident Response Centre (CCIRC) monitors the cyber threat environment around the clock and is responsible for coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber incidents. The Centre is a part of the [Government Operations Centre](#) and a key component of the government's all-hazards approach to national security and emergency preparedness.



- CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals and managers of [critical infrastructure](#) and other related industries.

# Singapore Government : SITSA



The screenshot shows the Singapore Government website with the SITSA announcement. The header includes the Singapore Government logo and navigation links. The left sidebar lists various categories like News, Events, and Publications. The main content area features a 'Press Releases' section dated 30 September 2009, titled '1 October 2009: Singapore Infocomm Technology Security Authority Set Up to Safeguard Singapore against IT Security Threats'. The text describes the establishment of SITSA on 1 Oct 2009 to safeguard Singapore against infocomm technology (IT) security threats. It outlines SITSA's mission to secure Singapore's IT environment, especially vis-à-vis external threats to national security such as cyber-terrorism and cyber-espionage. The announcement is divided into four numbered points detailing SITSA's responsibilities, the role of the National Infocomm Security Committee (NISC), and SITSA's areas of focus.

**30 September 2009**

**1 October 2009: Singapore Infocomm Technology Security Authority Set Up to Safeguard Singapore against IT Security Threats**

SITSA Singapore Infocomm Technology Security Authority (SITSA) will be set up on 1 Oct 2009 to safeguard Singapore against infocomm technology (IT) security threats. SITSA will be the national specialist authority overseeing operational IT security. SITSA's mission is to secure Singapore's IT environment, especially vis-à-vis external threats to national security such as cyber-terrorism and cyber-espionage.

2 SITSA will be responsible for operational IT security development and implementation at the national level. Regulatory agencies will continue to be responsible for IT security-related implementation for their sectors in coordination with SITSA. In the case of the Government and Infocomm sectors, this responsibility will continue to rest with Infocomm Development Authority of Singapore (IDA) in its capacity as the Government Chief Information Office (GCIO) and the government agency responsible for the Infocomm sector. Similarly, other regulatory agencies will continue to be responsible for IT security in their respective sectors.

3 The National Infocomm Security Committee (NISC) will remain as the national platform to formulate IT security policies and set strategic directions at the national level. IDA will continue to serve as secretariat to the NISC and also to promote Singapore as a secure and trusted hub.

4 SITSA will be a division within the Internal Security Department (ISD) of the Ministry of Home Affairs. SITSA's areas of focus will include:

- IT Security Consultancy for strategic Government projects that have national security impact
- Partnership Development to build relationships with key entities strategic to enhancing Singapore's IT security
- Critical Infocomm Infrastructure Protection to systematically harden the CIs in nationally critical sectors
- Technology Development to develop and maintain SITSA's technical competencies and to provide insights on developments in IT security and threats
- Singapore's planning and preparedness, and response, against any major external cyber attack

**SITSA's initiatives to harden critical national IT infrastructure and raise national preparedness against external cyber attacks**



# South Korea Government: KISA



# KISA : Korea Internet & Security Agency

- KISA(Korea Internet & Security Agency) was established as the public corporation responsible for managing the Internet of Korea on July 23th, 2009, by merging three institutes NIDA, KISA, and KIICA.
  - NIDA(National Internet Development Agency of Korea)
  - KISA(Korean Information Security Agency)
  - KIICA(Korea IT International Cooperation Agency)
- KISA has the following roles:
  - Protects Internet infrastructure from hacking cyber-terror, spam and other malicious activities
  - Operates krCERT CC (Korea Computer Emergency Response Team Coordination Center) to improve Internet security in Korea
  - Supporting international organizations such as ITU and OECD and assisting Korean IT companies
  - Specifically, KISA manages the Internet address resources such as IP address and .kr domain name as the national NIC (Network Information Center), and also researches for the next generation Internet address resources of Korea.






# Latin America : CITELE/OAS

- Within Latin America & Caribbean, CITELE and the OAS are working together on Regional Cybersecurity Strategy & Plans with ITU support:
- CITELE** = Inter-American Telecomms Commission
- OAS** = Organisation of American States



Organización de los Estados Americanos  
Organização dos Estados Americanos  
Organisation des États Américains  
Organization of American States

 [Antigua and Barbuda](#)

 [Costa Rica](#)

 [Haiti](#)

 [Saint Lucia](#)

 [Argentina](#)

 [Cuba](#)<sup>1</sup>

 [Honduras](#)<sup>2</sup>

 [Saint Vincent and the Grenadines](#)

 [Barbados](#)

 [Dominica \(Commonwealth of\)](#)

 [Jamaica](#)

 [Suriname](#)

 [Belize](#)

 [Dominican Republic](#)

 [Mexico](#)


 [The Bahamas \(Commonwealth of\)](#)

 [Bolivia](#)

 [Ecuador](#)

 [Nicaragua](#)

 [Trinidad and Tobago](#)

 [Brazil](#)

 [El Salvador](#)

 [Panama](#)

 [United States of America](#)

 [Canada](#)

 [Grenada](#)

 [Paraguay](#)

 [Uruguay](#)


 [Chile](#)

 [Guatemala](#)

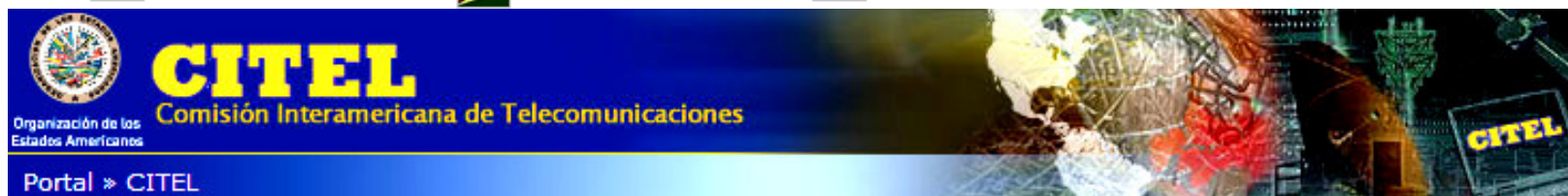
 [Peru](#)

 [Venezuela \(Bolivarian Republic of\)](#)

 [Colombia](#)

 [Guyana](#)

 [Saint Kitts and Nevis](#)



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica




International  
Telecommunication  
Union

Committed to connecting the world



# European Union : ENISA



Site Map | Accessibility | Contact | Legal Notice

Search Site

Home | About ENISA | **Our Activities** | Publications | Press & Media | Events | Public Procurement | Recruitment

you are here: home → our activities → cert

**CERT**  
What's new  
Overview  
Support  
Other work  
Events  
About us

## CERT


— filed under: [Training](#), [Information Sharing](#), [Incident Response](#), [Good Practice](#), [CERT](#), [Cooperation](#), [Exercises](#), [Incident Reporting](#), [CIIP](#)

### ENISA's work in the field of CERTs / CSIRTs

#### What is it all about?


##### CERT (Computer Emergency Response Team)

Computer Emergency Response Teams (CERTs, aka CSIRTs) are the key tool for Critical Information Infrastructure Protection (CIIP). Every single country that is connected to the internet must have capabilities at hand to effectively and efficient respond to information security incidents. But CERTs must do much more: they must act as primary security service providers for government and citizens, act as awareness raisers and educators.




Not every country connected to the internet disposes of CERT capabilities. And the level of maturity among those who do vary dramatically. It is ENISA's mission to as much as we can clear out the "white spots" on the CERT worldmap and to minimise the gaps by facilitating setting-up, training and exercising of CERTs.

#### videos




View or download the CERT Exercise video

#### related sites



Asian Pacific CERT



CERT Coordination Centre

# \* Workshop Session 2 \*

## The Need for Action!

<b>1 – Aim: Jamaican Action Plan</b>	<b>2 – Cybersecurity Costs</b>	<b>3 – Annual Cyber-Budgets</b>
<b>4 – Cybersecurity Benefits</b>	<b>5 – Benefits: Critical Sectors</b>	<b>6 – National Case Studies</b>
<b>7 – Jamaican Cyber Strategy</b>	<b>8 – ITU GCA Strategic Pillars</b>	<b>9 – Organisational RoadMap</b>



# Jamaican Cyber Strategy Plan

- 1) *Strategy*: Define & Communicate National Cyber Strategy
- 2) *Agency*: Establish National Cybersecurity Agency (NCA)
- 3) *Upgrades*: Roll-Out cybersecurity reviews and upgrades for all government ministries, agencies & institutions
- 4) *Budgets*: Determine Investment & Operational Budgets
- 5) *CIIP*: Work with representatives of all the Critical Service Sectors to define & implement cybersecurity action plans
- 6) *Awareness*: Roll-out national cybersecurity awareness campaign to all stakeholders including citizens & business
- 7) *Skills*: Establish professional cybersecurity skills training



# \* Workshop Session 2 \*

## The Need for Action!

1 – Aim: Jamaican Action Plan	2 – Cybersecurity Costs	3 – Annual Cyber-Budgets
4 – Cybersecurity Benefits	5 – Benefits: Critical Sectors	6 – National Case Studies
7 – Jamaican Cyber Strategy	8 – ITU GCA Strategic Pillars	9 – Organisational RoadMap



# ITU GCA Strategic Pillars

*We'll consider each of the ITU GCA strategic pillars in-depth during our 3-day cybersecurity workshop:*

- 1) Legal & Regulation Measures – Tues @ 9:30
- 2) Technical & Process Measures – Tues @ 11:30
- 3) Organisational Structures – Weds @ 9:30
- 4) Capacity & Skills Building – Weds @ 11:30
- 5) International Collaboration – Weds @ 12:15

*We'll then develop an outline Jamaican Cybersecurity Roadmap!...*



# \* ITU Cybersecurity Strategy \*

## "3-Day Workshop Overview"

<b>S1- Mon: 9:30-11:00</b>  <b>"The Cybersecurity Challenge!..."</b>	<b>S2-Mon: 11:30-13:00</b>  <b>"The Need for Action!"</b>	<b>S3 - Mon:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Cybersecurity Action Plans"</b>	<b>S4 - Mon:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Cybersecurity Action Plans"</b>
<b>S5- Tues: 9:30-11:00</b> <b>ITU Cyber Agenda: 1</b> <b>"Cybercrime and Legislation"</b>  <b>* Legal *</b>	<b>S6-Tues: 11:30-13:00</b> <b>ITU Cyber Agenda: 2</b> <b>"Technological Risks and Solutions"</b>  <b>* Technical *</b>	<b>S7 -Tues:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Legislation and Regulations"</b>	<b>S8 -Tues:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Legislation and Regulations"</b>
<b>S9- Wed: 9:30-11:00</b> <b>ITU Cyber Agenda: 3</b> <b>"Cybercrime and Organizational Structures"</b>  <b>* Organisation *</b>	<b>S10-Wed:11:30-13:00</b> <b>ITU Cyber Agenda: 4&amp;5</b> <b>"Capacity Building and Collaboration"</b>  <b>* Capacity &amp; Collaboration *</b>	<b>S11-Wed:14:00-15:30</b> <b>Group Session:</b>  <b>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</b>	<b>S12-Wed:16:00-17:30</b> <b>Group Session:</b>  <b>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</b>



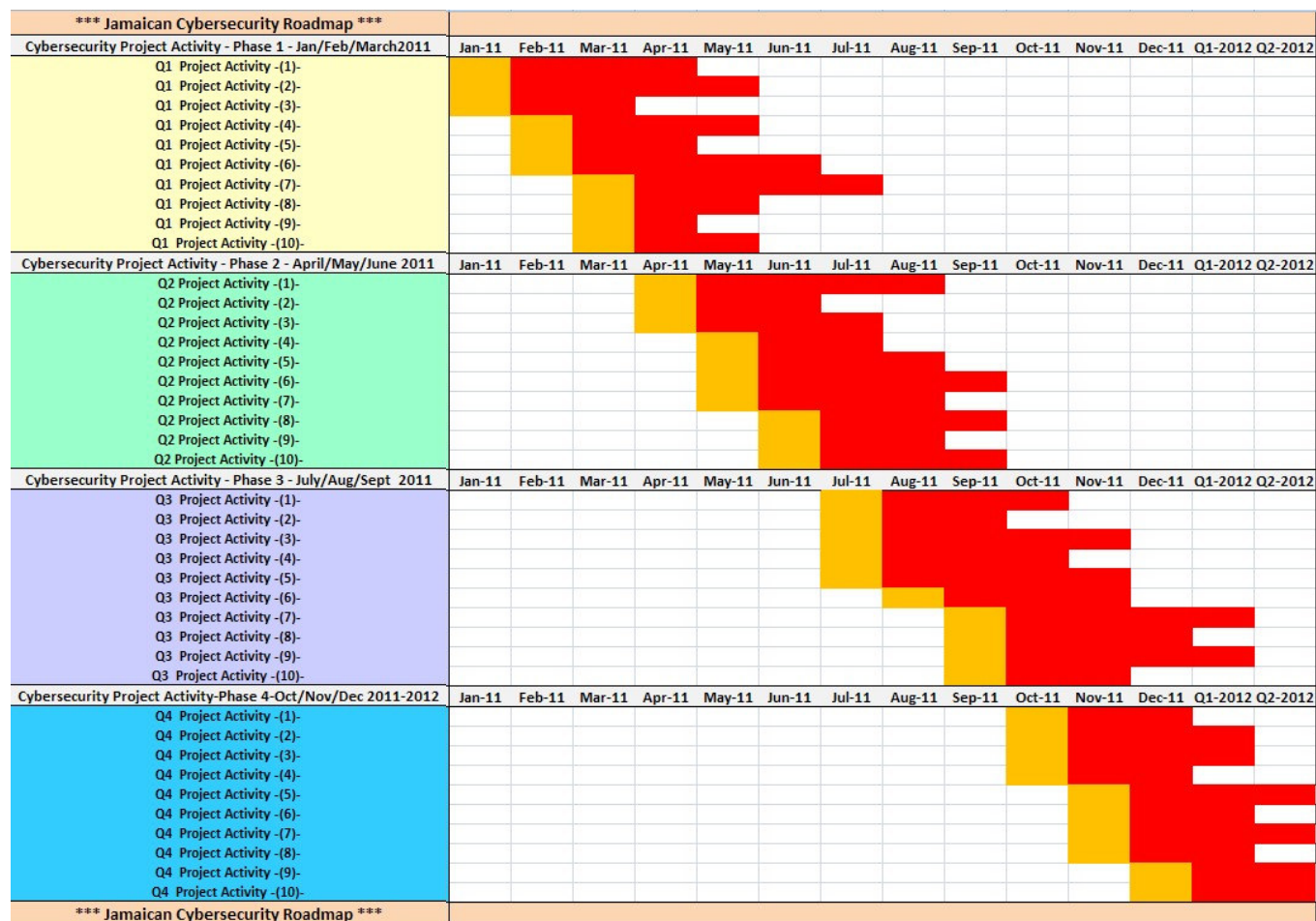
# \* Workshop Session 2 \*

## The Need for Action!

<b>1 – Aim: Jamaican Action Plan</b>	<b>2 – Cybersecurity Costs</b>	<b>3 – Annual Cyber-Budgets</b>
<b>4 – Cybersecurity Benefits</b>	<b>5 – Benefits: Critical Sectors</b>	<b>6 – National Case Studies</b>
<b>7 – Jamaican Cyber Strategy</b>	<b>8 – ITU GCA Strategic Pillars</b>	<b>9 – Organisational RoadMap</b>



# Jamaican Cybersecurity RoadMap



# Critical Sectors: *Cyber RoadMaps*

Each Critical Service Sector such as Banking, Telecommunications and Energy will require its own Cyber Strategy, Action Plan & Roadmap:

- During the Group Work Sessions we'll work in teams to develop Strategies, Actions and Activities that are relevant for each sector...
- We'll also work together on the Laws, Policies & Regulations that are required to significantly reduce Cybercrime, Cyber terrorism & Attacks...



# Example of National Cybersecurity Action Plan: Short-Term

# Action	SHORT-TERM ACTION PLAN: APRIL – SEPTEMBER 2011
1	<b>Government Cybersecurity Accountability</b> Consider making cybersecurity one of the Government's main management accountabilities with clear success criteria.
2	<b>Appoint National Cybersecurity Coordinator</b> Consider designating a senior Government Aide as National Cybersecurity Coordinator. The official should coordinate cybersecurity activities across the Government and report to the appropriate national bodies
3	<b>Complete and Promulgate National Cybersecurity Strategy</b> Consider using the template from the ITU Guidelines as a starting point for the National Cybersecurity Strategy. The Strategy should have clear roles and responsibilities, priorities, timeframes and performance metrics. Thereafter, obtain Government approval for the Cybersecurity Strategy.
4	<b>Create National Cybersecurity Coordination Agency</b> In common with other countries, consider creating a multi-agency body as a focal point for all activities dealing with protecting 's cyberspace against threats such as cybercrime.
5	<b>Define National Cybersecurity Framework</b> The framework should be flexible to allow stakeholder organisations to achieve the stated goals in the most efficient and effective manner.
6	<b>Initiate Public-Private Sector Cybersecurity partnership</b> The process should be transparent and consider all views.
7	<b>Create Computer Incident Response Team (CIRT)</b> Consider creating a national CIRT to analyse cyber threat trends, improve response coordination and dissemination of information across the Government, to industry, citizens and international partners.
8	<b>Strengthen Legal and Regulatory System</b> Complete the Cybercrime Legislation Programme and enforce the new laws.
9	<b>Initiate Cybersecurity Awareness and Education campaign</b> Consider working with the private sector and civil society to explain cyber threats to the citizens and their role in defending cyberspace.
10	<b>Define and initiate Cybersecurity Skills and Training Programme</b> Consider the experience of other countries in creating a cybersecurity skills and training programme with periodic measurement of skills.





# Example of National Cybersecurity Action Plan: Mid-Term

# Action	MID-TERM ACTION PLAN: OCTOBER 2011 – JANUARY 2012
1	Define, localise and communicate Government cybersecurity Standards in areas such as Data Classification and Staff Vetting and Clearance.
2	The National Cybersecurity Agency (NCA) should ensure that cybersecurity policies are in line with the new Cybercrime legislation
3	Launch cybersecurity awareness campaign across Government and NCA website for government, commercial and educational sectors with guidelines, standards and training materials.
4	As National Technical Authority for Information Assurance, the NCA should advise on how to secure eGovernment Services.
5	Use formal channels to organise study trips for NCA Staff to other Cybersecurity Agencies
6	Conduct in-depth cybersecurity review and audit of Government ministries, agencies and associated bodies.
7	Review Physical Security of organisations hosting critical infrastructure.
8	Parliamentary review of the proposed National Cybersecurity Act 2011
9	NCA Programme on Business Continuity and Disaster Recovery
10	Develop and Resource the national CIRT/CERT. In addition, develop national Cyber Incident Response Framework involving public-private stakeholders. Also develop, test and exercise incident response plans for Government emergency communications during natural disasters, cyberattacks, crisis or war as required by the National Security Concept.
11	Implement six to nine months' programme of Operational Cybersecurity upgrades. The activities may extend into 2011 and beyond.
12	Ensure that the Government Communications Network and all new services comply with the agreed Government Authentication Framework.
13	Launch the Cybersecurity Skills and Training Programme for cybersecurity professionals and collaborate with commercial and educational sectors to boost cybersecurity Research and Development.
14	Secure Parliamentary, Cabinet & Government approval of the Cybersecurity Act 2011 and associated Cybercrime legislation.
15	Organise an annual Regional Cybersecurity Conference to communicate progress, share views and promote national Cybersecurity Programme.



# ITU Self-Assessment Toolkit: Critical Information Infrastructure Protection - CIIP



## ITU National Cybersecurity/CIIP Self-Assessment Tool

ICT Applications and Cybersecurity Division  
Policies and Strategies Department  
ITU Telecommunication Development Sector

April 2009 Revised Draft

For further information, please contact the  
ITU-D ICT Applications and Cybersecurity Division at <cybmail@itu.int>



**ITU Centres of Excellence Network for the Caribbean Region**  
**Developing a National and Organizational Cybersecurity Strategy**  
*13-15 September, Kingston, Jamaica*



University of Technology,  
Jamaica



*Committed to connecting the world*

# Initial Actions: National Cybersecurity

**ACTION ITEM: Prepare a brief statement of each of these points:**

1. The role of ICTs in the nation:
  - a. In the economy
  - b. In the national security
  - c. In the critical infrastructures
  - d. In the social interaction (civil society and social discourse)
2. Risks and ICTs in the nation:
  - a. Identify threats from and vulnerabilities of ICT use
  - b. Identify risks
    - i. To the economy
    - ii. To the national security
    - iii. To the critical infrastructures
    - iv. To the social interaction (civil society and social discourse)
3. The place of cybersecurity/CIIP in overall national objectives and concerns
4. Policy on cybersecurity/CIIP
  - a. Goals
  - b. How will it be implemented
  - c. Timeframes
  - d. Metrics
  - e. Relationship to regional and international activities



# Actions: National CIIP Participants

## ACTION ITEM: Identify national participants in cybersecurity/CIIP:

1. **Government:** For each government ministry/agency with a role in cybersecurity/CIIP:
  - a. Identify the ministry/agency.
  - b. Describe its role(s) in the development of policy and in operations of cybersecurity/CIIP related to the economy, national security, CII and social interaction.
  - c. Identify a point of contact for each entity and for each significant role.
2. **Other participants:** For each non-government participant with a role in cybersecurity/CIIP including industry, civil society, academia and others, identify key individual firms and institutions, critical sector groupings, associations, and other key entities and groupings within the nation with a role in cybersecurity/CIIP.
  - a. Identify the participant.
  - b. Describe its role(s) in the development of policy and in operations of cybersecurity/CIIP related to the economy, national security, CII and social interaction.
  - c. Identify a point of contact for each entity and for each significant role.



# Actions: Cyber Policy and Operations

## ACTION ITEM: Policy and operational forum/structures.

1. Identify the government institution(s) designated to lead the national cybersecurity/CIIP effort for policy development and operations.
2. Policy development: Identify relevant forum/structure for use by the lead agency for the development of cybersecurity/CIIP policy.
  - a. Name of forum/structure.
  - b. Participants.
  - c. Role and objective of forum/structure.
  - d. How is input from other participants obtained and addressed?
  - e. Evaluate forum/structure for adequacy and identify required modifications.
3. Operations: Identify relevant forum/structures available to enhance operational cybersecurity/CIIP. Include government and non-government forums and structures.
  - a. Name of forum/structure.
  - b. Who leads and convenes the forum/structure?
  - c. Participants.
  - d. Role and objective of forum/structure.
  - e. Is forum/structure trusted? If yes, how is trust addressed?
  - f. Evaluate forum/structures for adequacy and identify required modifications.





# Cybersecurity: Public & Private Sector Partnership (PPP)

**ACTION ITEM: Describe actions taken and requirements for future action to develop government/private sector collaboration that will;**

1. Include private sector perspectives in all stages of the development and implementation of cybersecurity/CIIP policy.
2. Establish cooperative arrangements between government and the private sector for information sharing and incident management.
3. Bring private sector groups and government together in trusted forums to address common cybersecurity/CIIP challenges.
4. Encourage cooperation among participants in each critical infrastructure to address common cybersecurity/CIIP interests.
  - a. How is government involved in this collaboration?
5. Encourage cooperation among participants from interdependent critical infrastructures to address shared cybersecurity/CIIP interests.
  - a. How is government involved in this collaboration?



# Actions: CIIP Incident Response

**ACTION ITEM: Describe actions taken and requirements for future action in regard to the incident management capability function to prevent, prepare for, respond to, and recover from cybersecurity/CIIP incidents:**

1. Identify agency to provide the incident management capability function for watch, warning, response and recovery.
2. Identify cooperating government agencies and points of contact for each.
3. Identify cooperating participants (industry, CII, and civil society partners) and points of contact for each.
4. Identify arrangements for cooperation and information sharing between the incident management capability and its cooperating partners.
5. Identify international cooperating partners, points of contact and arrangements for cooperation.
6. Ensure availability of CIRT services by:
  - a. Identifying available and/or contracting with existing CIRTs.
  - b. Establishing a CIRT with national responsibility.
7. Develop tools and procedures for the protection of the cyber resources of government entities.
8. Develop procedures and tools for the dissemination of incident management information.
9. Develop an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity/CIIP.
10. Assess and periodically reassess the current state of cybersecurity/CIIP efforts and develop program priorities.
11. How will incident management capability and cybersecurity/CIIP effort be funded and staffed?



# Actions: Update National Legislation

**ACTION ITEM: Describe actions taken and requirements for future action in regard to the review and update of the national legal infrastructure:**

1. Cybercrime authorities and procedures.
  - a. Review and update legal authorities.
  - b. Establish or identify national cybercrime units.
  - c. Participate in international efforts, such as the 24/7 Cybercrime Point of Contact Network.
  - d. Develop an understanding among prosecutors, judges, and legislators of cybercrime issues.
2. Other legal infrastructures.
  - a. Which ones have been addressed?
  - b. Which ones require review?



# Actions: Cybersecurity Cultural Awareness

**ACTION ITEM: Describe actions taken and requirements for future action to develop a national culture of cybersecurity: including, for example;**

1. To implement a cybersecurity plan for government-operated systems.
2. To promote a comprehensive national awareness program so that all participants – businesses, the general workforce, and the general population – secure their own parts of cyberspace and participate effectively in a new culture of cybersecurity.
3. To support outreach with special attention to the needs of children and individual users.
4. To enhance Science and Technology (S&T) and Research and Development (R&D) activities.
5. To identify national cybersecurity/CIIP training requirements and how to achieve them.



# Summary: National Cybersecurity Action Plan and RoadMap

**ACTION ITEM: Review responses in Sections 1-7 and prepare statements that respond to the following points. When combined these statements should represent a draft national strategy on cybersecurity/CIIP for your country:**

## 1. From Section 1 (A Case for National Action):

- Identify a national policy on cybersecurity/CIIP.
- Identify a case for national action on cybersecurity/CIIP.

## 2. From Section 2 (Participants in the National Response):

- Identify key government ministries and agencies with leadership responsibilities in cybersecurity/CIIP and describe their roles.
- Identify key other participants with responsibilities in cybersecurity/CIIP and describe their role(s).

## 3. From Section 3 (Organizing for Cybersecurity/CIIP):

- Identify organizational structures to be used for the development of cybersecurity/CIIP policy.
  - Describe the workings of these structures and the involvement of other participants.
- Identify organizational structures to be used for ongoing cybersecurity/CIIP operations.
  - Describe the workings of these structures and the involvement of other participants.

## 4. From Section 4 (Government-Private Sector Collaboration):

- Identify objectives and structures for government/private sector collaboration.
- Identify objectives and structures for trusted government/private sector collaboration.

## 5. From Section 5 (Incident Management Capabilities):

- Identify location within government of the incident management capability function.
- Identify and prioritize objectives of the incident management capability function.

## 6. From Section 6 (Legal Infrastructures):

- Identify objectives for updating the legal infrastructure related to cybercrime.
- Identify objectives for updating other elements of the legal infrastructure.

## 7. From Section 7 (Culture of Cybersecurity):

- Identify and prioritize objectives for building a national culture of cybersecurity.

## 8. Additional Requirements:

- Identify how the national strategy will be finalized and promulgated.
- Review funding requirements and sources for each element of the national strategy.
- Identify implementation timeframes.
- Identify metrics and reassessment objectives.





# \* ITU Cybersecurity Strategy \*

## "3-Day Workshop Overview"

<b>S1- Mon: 9:30-11:00</b>  <b>"The Cybersecurity Challenge!..."</b>	<b>S2-Mon: 11:30-13:00</b>  <b>"The Need for Action!"</b>	<b>S3 - Mon:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Cybersecurity Action Plans"</b>	<b>S4 - Mon:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Cybersecurity Action Plans"</b>
<b>S5- Tues: 9:30-11:00</b>  <b>ITU Cyber Agenda: 1</b> <b>"Cybercrime and Legislation"</b>	<b>S6-Tues: 11:30-13:00</b>  <b>ITU Cyber Agenda: 2</b> <b>"Technological Risks and Solutions"</b>	<b>S7 -Tues:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Legislation and Regulations"</b>	<b>S8 -Tues:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Legislation and Regulations"</b>
<b>S9- Wed: 9:30-11:00</b>  <b>ITU Cyber Agenda: 3</b> <b>"Operational Risks and Organisational Structures"</b>	<b>S10-Wed:11:30-13:00</b>  <b>ITU Cyber Agenda: 4&amp;5</b> <b>"Capacity Building and Collaboration"</b>	<b>S11-Wed:14:00-15:30</b> <b>Group Session:</b>  <b>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</b>	<b>S12-Wed:16:00-17:30</b> <b>Group Session:</b>  <b>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</b>



# \* Group Workshop Session 3 \*

## Developing Cybersecurity Action Plans

# Action	SHORT-TERM ACTION PLAN: January - June 2011
1	<b>Action Title</b> Action Description
2	<b>Action Title</b> Action Description
3	<b>Action Title</b> Action Description
4	<b>Action Title</b> Action Description
5	<b>Action Title</b> Action Description
6	<b>Action Title</b> Action Description
7	<b>Action Title</b> Action Description
8	<b>Action Title</b> Action Description
9	<b>Action Title</b> Action Description
10	<b>Action Title</b> Action Description



# \* Group Workshop Session 3 \*

## Developing Cybersecurity Action Plans

- Team Worksheet – Cybersecurity Action Plans
  - *Task 1* – Choose Critical Sector: Banking, Energy, Government, Healthcare, Education
  - *Task 2* – Identify and Discuss the Potential Cyber Threats and Risks to your Sector
  - *Task 3* – Evaluation the Impact and Economic Damage of such Cyber Threats & Risks
  - *Task 4* – Brainstorm the Possible Management Actions to Combat these Risks
  - *Task 5* – Structure and Prioritise the chosen Actions for the Critical Sector
  - *Task 6* – Complete the Cybersecurity Action Plan Template
  - *Task 7* – Write a short presentation script & slides as CSO to “sell” your programme

*.....Focus on practical actions and think about the most efficient ways in which they can be delivered with the staff, technical and operational resources at your disposal!*

# Task Description: Government Sector

- 1) You have just been appointed as the new CSO (Chief Security Officer) for the Government working within the Prime Minister's Cabinet Office with top-level responsibility for cybersecurity across all aspects of Government.
- 2) Your task is to prepare a report & short presentation to the Cabinet regarding the technical and operational actions that should be taken across Government in order to provide an adequate defence against cyberthreats & potential attacks.
- 3) Assume that the Government comprises around 20 Ministries including Foreign Office, Home Office, Security, Defence, Transportation, Finance, Justice, Energy, Environment, Healthcare and Industry, as well as Regional Administrations
- 4) There is already a Government Data Network and various ICT computer centres and databases that are not yet secured against cyber threats & attacks

*.....Plan your security priorities, and prepare a practical cybersecurity action plan*

# Task Description: Banking/Finance Sector

- 1) You have just been appointed as the CSO (Chief Security Officer) for a major National Financial Institution with both retail & investment operations
- 2) Your task is to prepare a report and presentation for the Board of Management with recommendations on the technical and operational actions that should be taken across the Financial Group to provide security against cybercriminal attacks
- 3) Assume that the Bank includes a large national retail network of local branches and ATM machines, as well as on-line banking operations. Also assume that the investment banking operations are networked with several other major global banking networks and that stocks, bonds & commodities are traded in real-time
- 4) There have already been cybercriminal attacks on bank accounts & transactions in the past year and you are asked by the CEO to ensure that any future attacks are immediately detected, maybe with an in-house CERT, and any losses minimised

*.....Consider all the potential cyber threats and prioritise your action plan for the Board*





# Task Description: Telecomms/Mobile Sector

- You have just been appointed as the CSO (Chief Security Officer) for the National Telecommunications or Mobile Networking Carrier in Jamaica
- Your task is to prepare a full report and presentation to your Board of Management with recommendations for upgrading all aspects of cybersecurity, specifically focusing upon the technical and operational procedures & measures
- Assume that the National Telecomms and/or Mobile Operations comprises a national distributed radio and landline network with a range of traditional telecomms and broadband “new generation” IP technology switches & servers.
- You are responsible for ALL aspects of network security including the private leased line (VPN) networks for the government & large enterprises, as well as the telecomms ISP operations which includes Hosted eCommerce WebSites, VoIP & Gateways & Routers to other Regional and International Networks

*...Consider all the threats and prioritise your actions in order to minimise the risks and potential damage from future cyber attacks on the national telco network*

# Task Description: Transport/Airports Sector

- You have just been appointed the CSO (Chief Security Officer) for the country's largest international airport (Kingston), including both passenger and cargo operations, as well as associated regional airports (Montego Bay)
- Your task is to prepare a report and presentation to the Board of Management for the Airport with recommendations and action plan for the upgrading of all aspects of security across the airport/port operational and ICT facilities.
- Assume that the Airport has both airside and landside operations, with multiple domestic and international airlines flying routes to an intensive schedule. The ICT assets include the real-time air traffic control, passenger & cargo screening systems, staff and vehicle access, and the computerised dispatching network and baggage handling network.
- You are responsible as CSO for both the operational security and associated security staff as well as all the cybersecurity aspects of the airport operation.

*...Consider all the possible cybercriminal and cyberterrorist threats to the airport facilities and prioritise your action plan to minimise risks from potential attacks*



# Task Description: Energy/Utilities Sector

- You have recently been appointed as the CSO (Chief Security Officer) for the National Energy and Power Grid which provides most of the nation's energy
- Your task is to prepare a report and presentation for the Board of Management with recommendations and action plan for upgrading all aspects of security with respect to the National Power Grid and its regional centres and operations
- Assume that the National Power Grid and Company has several large power stations (non-nuclear) and distribution network across cities, towns & villages. The ICT computer facilities include all the power station process control networks & applications, as well as the 24/7 real-time management of energy (electricity & gas flow) through the national power grid to business & end-users
- You are responsible as CSO for both the technical aspects of ICT cybersecurity as well as operational security for the power stations, offices and other facilities

*....Consider all the possible cyberthreats and cyberterrorism that could impact the national grid and prioritise a practical plan that minimises the risk of attack, and reduces the collateral damage and disruption following any major power failure*



# \* Group Workshop Session 3\*

## Developing Cybersecurity Sector Action Plans

### Suggested Time Allocations for Task Actions: 90mins

<b>1 – Task Assignment: Choose your Critical Service Sector:</b>  <i>Government, Banking/Finance Telecomms, Transport, Energy</i>	<b>Task 2 – Define Cyberthreats</b>	<b>Task 2 – Define Cyberthreats</b>
<b>Task 3 – Evaluate the Potential Impact &amp; Economic Damage from your list of cyberthreats</b>	<b>Task 4 – Discuss Management Actions to Combat &amp; Defend against these Cyber Risks</b>	<b>Task 5 – Structure &amp; Prioritise Actions for your Critical Sector</b>  <i>(Colour-Code Actions by the 5 ITU GCA Cybersecurity Strategy Pillars)</i>
<b>Task 6 – Complete the Sector Cybersecurity Actions Plans for the Short &amp; Mid-Term: 2011</b>	<b>Task 7– Prepare Short 10 Min Presentation of Action Plans</b>	<b>Task 7 – Prepare Short 10min Presentation of Action Plans</b>

**Note: Each Task Time Segment = 10Mins**

# Key to Cybersecurity Workshop Session

## Colour-Code Classifications: Interactive Tasks

Colour Code Workshop	RED	ORANGE	YELLOW	BLUE	GREEN
<b>Monday</b> <b>-Action Plans -</b>	(1) Legal	(2) Technical	(3) Organisation	(4) Capacity	(5) International
<b>Tuesday</b> <b>- Laws -</b>	Information Disclosure	Computer Misuse	Forgery & ID Fraud	Information Interception	Copyright & Patents Law
<b>Wednesday</b> <b>- Road Map -</b>	Q1-2011	Q2-2011	Q3-2011	Q4-2011	FY2012
<b>Thursday</b> <b>- ICT Security-</b>	Unauthorised Info Access	DDoS-Denial of Services	MALWARE	Disclosure & Misuse	Info Access & Exploitation
<b>Friday</b> <b>- Sector Security -</b>	Cyber Criminal Threat	Cyber Terrorist Threat	Malicious Hacking & Exploitation	Internal Operational Threat	Natural Disaster or Other Event





# \* ITU Cybersecurity Strategy \*

## "3-Day Workshop Overview"

<b>S1- Mon: 9:30-11:00</b>  <b>"The Cybersecurity Challenge!..."</b>	<b>S2-Mon: 11:30-13:00</b>  <b>"The Need for Action!"</b>	<b>S3 - Mon:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Cybersecurity Action Plans"</b>	<b>S4 - Mon:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Cybersecurity Action Plans"</b>
<b>S5- Tues: 9:30-11:00</b>  <b>ITU Cyber Agenda: 1</b> <b>"Cybercrime and Legislation"</b>	<b>S6-Tues: 11:30-13:00</b>  <b>ITU Cyber Agenda: 2</b> <b>"Technological Risks and Solutions"</b>	<b>S7 -Tues:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Legislation and Regulations"</b>	<b>S8 -Tues:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Legislation and Regulations"</b>
<b>S9- Wed: 9:30-11:00</b>  <b>ITU Cyber Agenda: 3</b> <b>"Operational Risks and Organisational Structures"</b>	<b>S10-Wed:11:30-13:00</b>  <b>ITU Cyber Agenda: 4&amp;5</b> <b>"Capacity Building and Collaboration"</b>	<b>S11-Wed:14:00-15:30</b> <b>Group Session:</b>  <b>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</b>	<b>S12-Wed:16:00-17:30</b> <b>Group Session:</b>  <b>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</b>



\* **Group Workshop Session 4\***  
**Team Discussion: Cybersecurity Sector Action Plans**  
**Schedule: Task Presentations = 90mins**

Group 1 = Government	Group 1 = Government	Group 2 = Banking/Finance
Group 2 = Banking/Finance	Group 3 = Telecomms/Mobile	Group 3 = Telecomms/Mobile
Group 4 = Transport or Energy	Group 4 = Transport or Energy	Group Discussion & Summary

**Note: Each Task Time Segment = 10Mins**

# \* ITU Cybersecurity Strategy \*

## *"3-Day Workshop Overview"*

<b>S1- Mon: 9:30-11:00</b>  <b>"The Cybersecurity Challenge!..."</b>	<b>S2-Mon: 11:30-13:00</b>  <b>"The Need for Action!"</b>	<b>S3 - Mon:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Cybersecurity Action Plans"</b>	<b>S4 - Mon:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Cybersecurity Action Plans"</b>
<b>S5- Tues: 9:30-11:00</b>  <b>ITU Cyber Agenda: 1</b> <b>"Cybercrime and Legislation"</b>	<b>S6-Tues: 11:30-13:00</b>  <b>ITU Cyber Agenda: 2</b> <b>"Technological Risks and Solutions"</b>	<b>S7 -Tues:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Legislation and Regulations"</b>	<b>S8 -Tues:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Legislation and Regulations"</b>
<b>S9- Wed: 9:30-11:00</b>  <b>ITU Cyber Agenda: 3</b> <b>"Operational Risks and Organisational Structures"</b>	<b>S10-Wed:11:30-13:00</b>  <b>ITU Cyber Agenda: 4&amp;5</b> <b>"Capacity Building and Collaboration"</b>	<b>S11-Wed:14:00-15:30</b> <b>Group Session:</b>  <b>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</b>	<b>S12-Wed:16:00-17:30</b> <b>Group Session:</b>  <b>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</b>



# \* Workshop Session 5 \*

## The Global Cybersecurity Agenda: *...Cybercrime & Legislation*

1 – Definition and Scope	2 – Dimensions of Cybercrime	3 – Cybercrimes against CIIP
4 – National Cybercrime Laws	5 – UK Cyber Legislation	6 – National Cyber Strategies
7 – ITU Cybercrime Toolkit	8 – Digital Forensics	9 – Legislation for Jamaica



# **\* Workshop Session 5 \***

## **The Global Cybersecurity Agenda: ...Cybercrime & Legislation**

<b>1 – Definition and Scope</b>	<b>2 – Dimensions of Cybercrime</b>	<b>3 – Cybercrimes against CIIP</b>
<b>4 – National Cybercrime Laws</b>	<b>5 – UK Cyber Legislation</b>	<b>6 – National Cyber Strategies</b>
<b>7 – ITU Cybercrime Toolkit</b>	<b>8 – Digital Forensics</b>	<b>9 – Legislation for Jamaica</b>





# Cybercrime & Legislation:

## - Definition & Scope -

- **Cybercrime:** Criminal activities that specifically target a *computer* or *network* for malicious damage, infiltration, extortion, theft & fraud.
- **Cyberterrorism:** Used for those cybercriminal acts that are deliberately targeted to create large-scale disruption of critical information infrastructure such as government, banking, energy & telecommunications networks
- **Cyberattacks:** Typical terms used to designate cyberattacks include: spamming, phishing, spoofing, pharming, denial of service, trojans, viruses, worms, malware, spyware and botnets.

Upgraded National Laws & Regulations are required to enable the civil & military enforcement agencies to investigate & prosecute cybercriminal & cyberterrorist activities that are illegal & disruptive against citizens, businesses and the state.



# ITU Toolkit for Cybercrime Legislation : February 2010



## ITU TOOLKIT FOR CYBERCRIME LEGISLATION



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world

# **\* Workshop Session 5 \***

## **The Global Cybersecurity Agenda: ...Cybercrime & Legislation**

<b>1 – Definition and Scope</b>	<b>2 – Dimensions of Cybercrime</b>	<b>3 – Cybercrimes against CIIP</b>
<b>4 – National Cybercrime Laws</b>	<b>5 – UK Cyber Legislation</b>	<b>6 – National Cyber Strategies</b>
<b>7 – ITU Cybercrime Toolkit</b>	<b>8 – Digital Forensics</b>	<b>9 – Legislation for Jamaica</b>

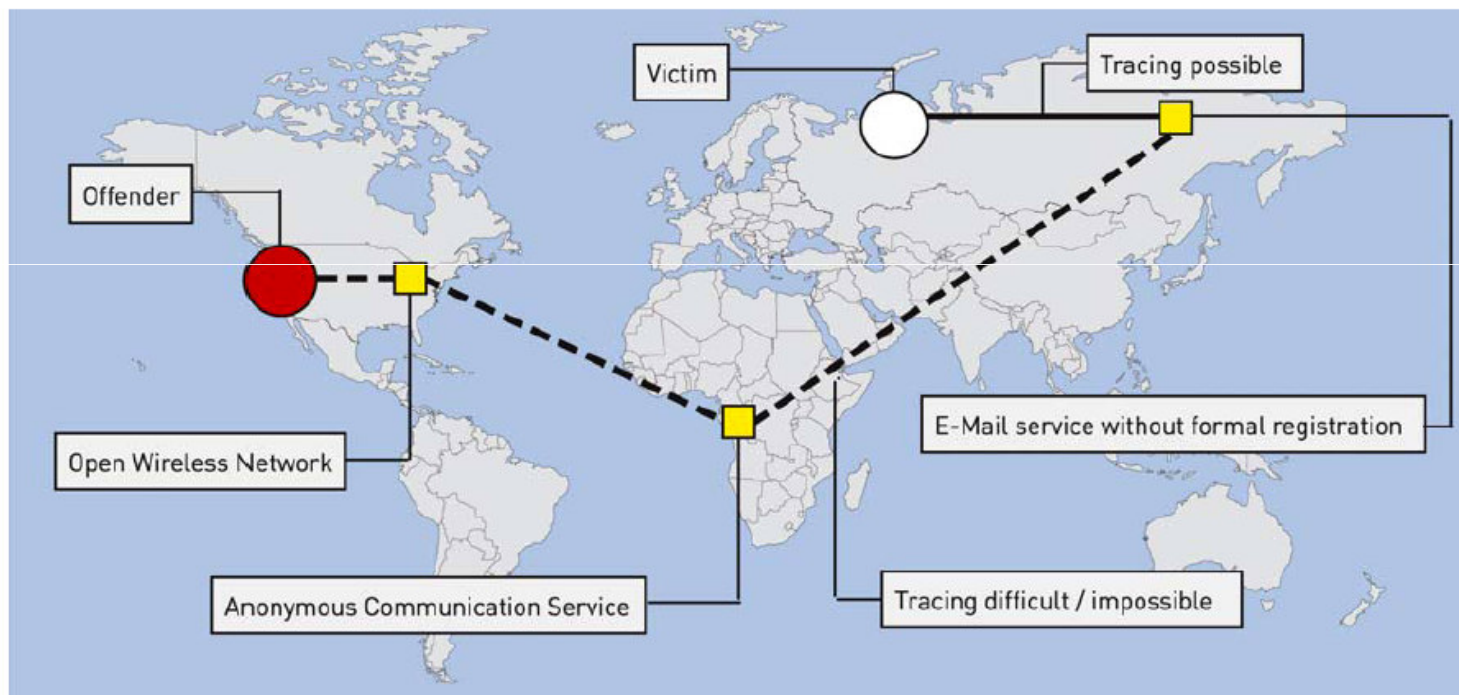


# Dimensions of Cybercrime

- Cybercrimes & Cyberterrorism cover many dimensions of illegal cyber activity including:
  - Unauthorised Access to Computers and Networks
  - Malicious Interference and Disruption of Systems
  - Distribution and Remote Management of Malware
  - Digital Forgery, Fraud, Gaming Scams and Financial Extortion
  - Theft of Information, Databases, Documents & related materials
  - Interception of wireless, mobile & wired network communications
  - Theft of personal identities (IDs), as well as RFID & Access Devices
  - Distributed Denial of Service Attacks using Global “Botnets”
  - Defacement & Manipulation of Websites, Databases & Documents



# ITU Guide on Cybercrime: 2009



## UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world

# Multi-Country Involvement in CyberAttacks

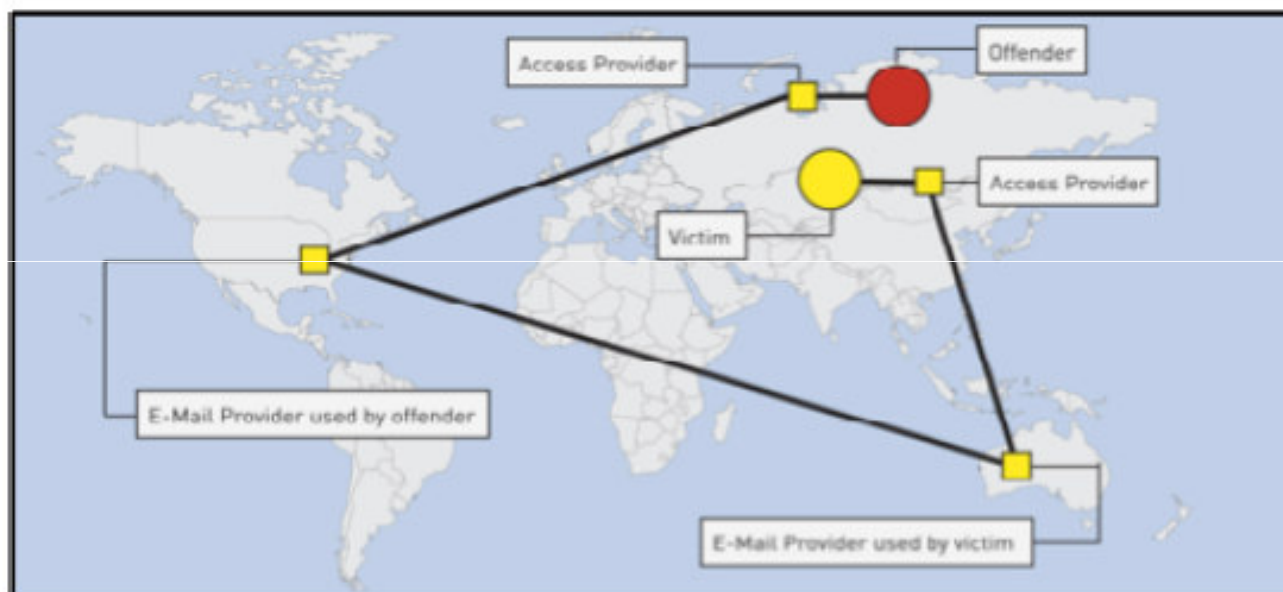


Figure 29

The graphic shows that, even if offenders and targets are based in the same country, the act of sending an email with illegal content can involve and cross various countries. Even if this is not the case, data transfer processes may be directed outside the country, before being redirected back.





# Independence of Location and Presence at the Crime Site



Figure 30

Offenders can access the Internet to commit offences from almost anywhere in the world. Issues that potential offenders take into account while deciding where to base themselves include: the status of cybercrime legislation, the effectiveness of law enforcement agencies and the availability of anonymous Internet access.



# Distributed Denial of Service (DDoS) using Spam Mail and “Botnets”



Figure 32

One example for automation processes is the dissemination of Spam. Millions of emails can be sent out within a short period of time.



# Malicious Activity by Country

Overall Rank 2009 2008		Country	Percentage 2009 2008		2009 Activity Rank				
					Malicious Code	Spam Zombies	Phishing Hosts	Bots	Attack Origin
1	1	United States	19%	23%	1	6	1	1	1
2	2	China	8%	9%	3	8	6	2	2
3	5	Brazil	6%	4%	5	1	12	3	6
4	3	Germany	5%	6%	21	7	2	5	3
5	11	India	4%	3%	2	3	21	20	18
6	4	United Kingdom	3%	5%	4	19	7	14	4
7	12	Russia	3%	2%	12	2	5	19	10
8	10	Poland	3%	3%	23	4	8	8	17
9	7	Italy	3%	3%	16	9	18	6	8
10	6	Spain	3%	4%	14	11	11	7	9

**Table 1. Malicious activity by country**

Source: Symantec Corporation



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world

# Cybercrime : Identity Theft

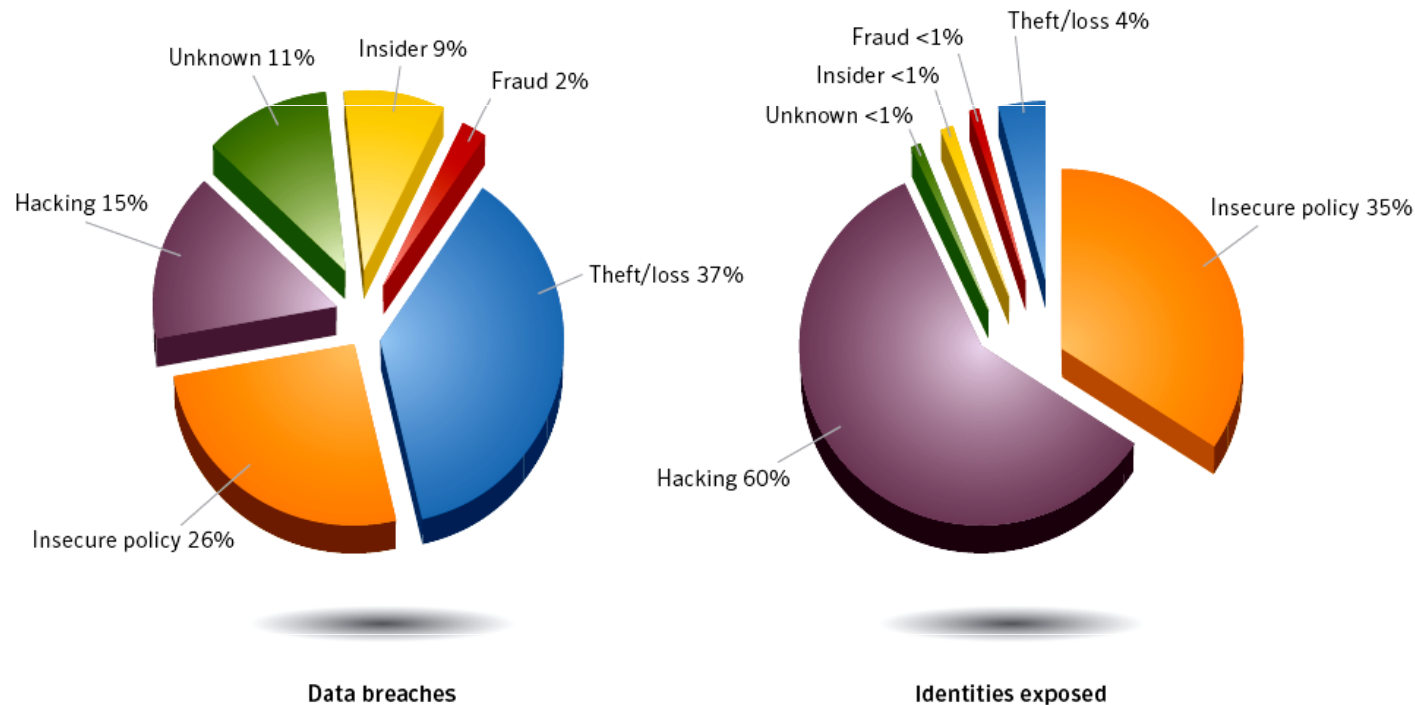


Figure 1. Data breaches that could lead to identity theft by cause and identities exposed<sup>12</sup>

Source: Based on data provided by OSF DataLoss DB

# Top Categories of Spam Mail

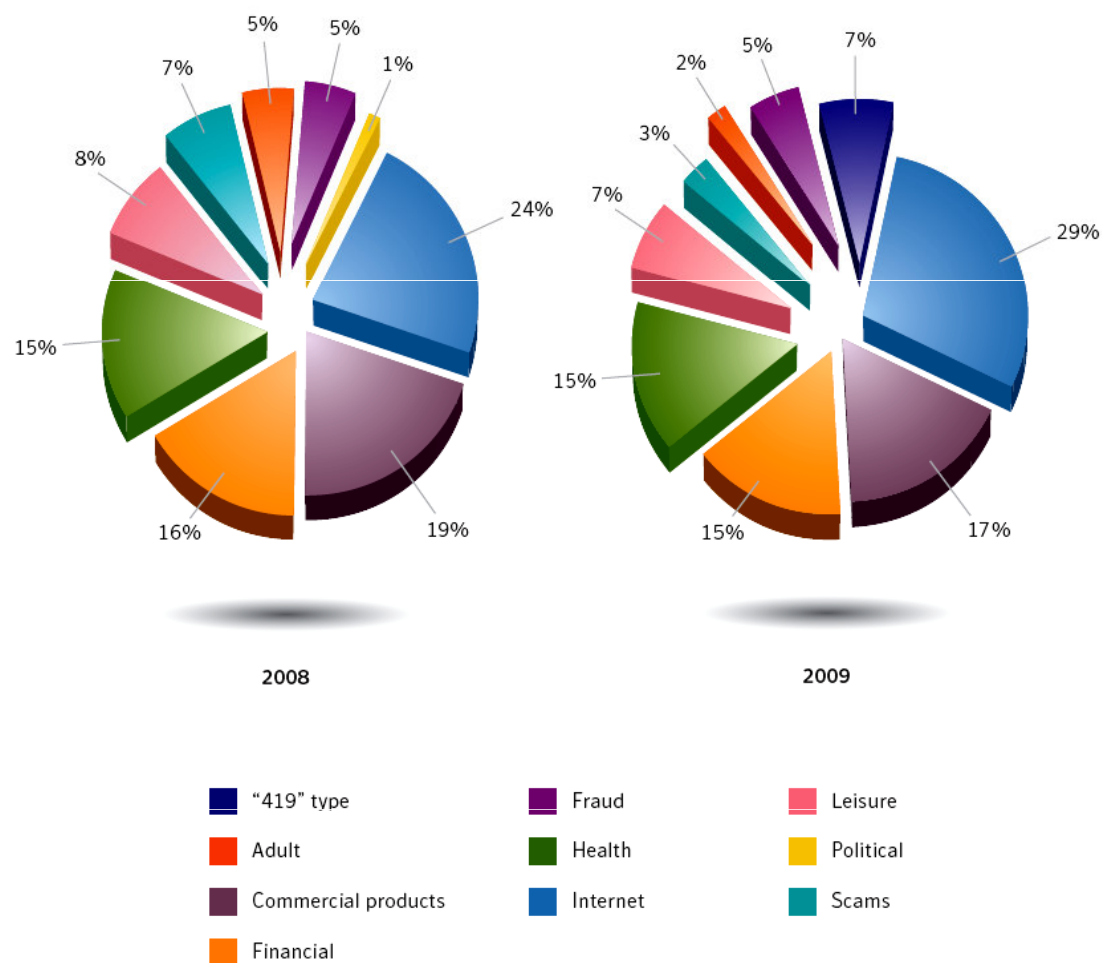
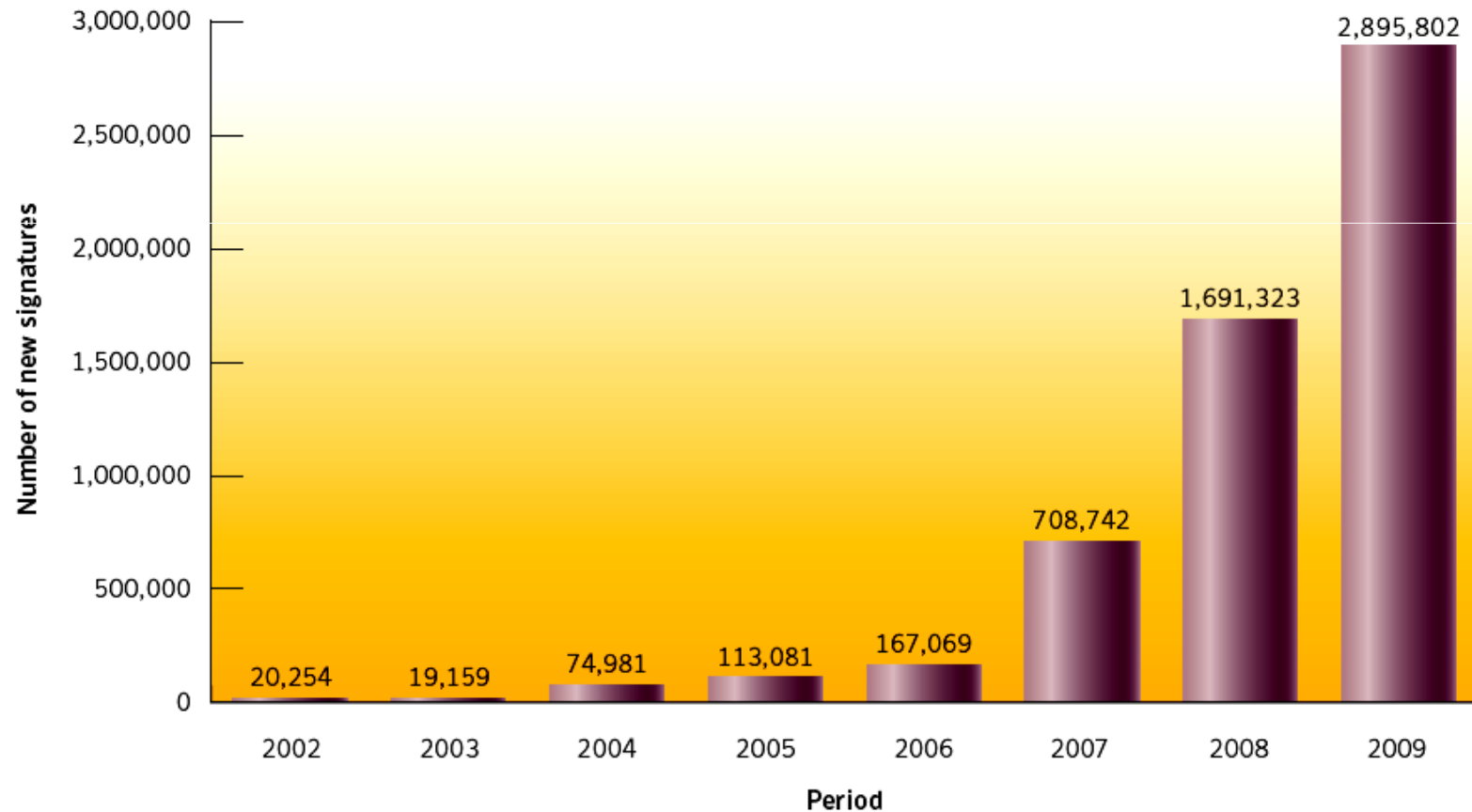


Figure 3. Top spam categories  
Source: Symantec

# Growth of Malicious Codes: 2002 - 2009



**Figure 10. New malicious code signatures**

*Source: Symantec.*



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



**Committed to connecting the world**



# Comparison of Malicious Codes

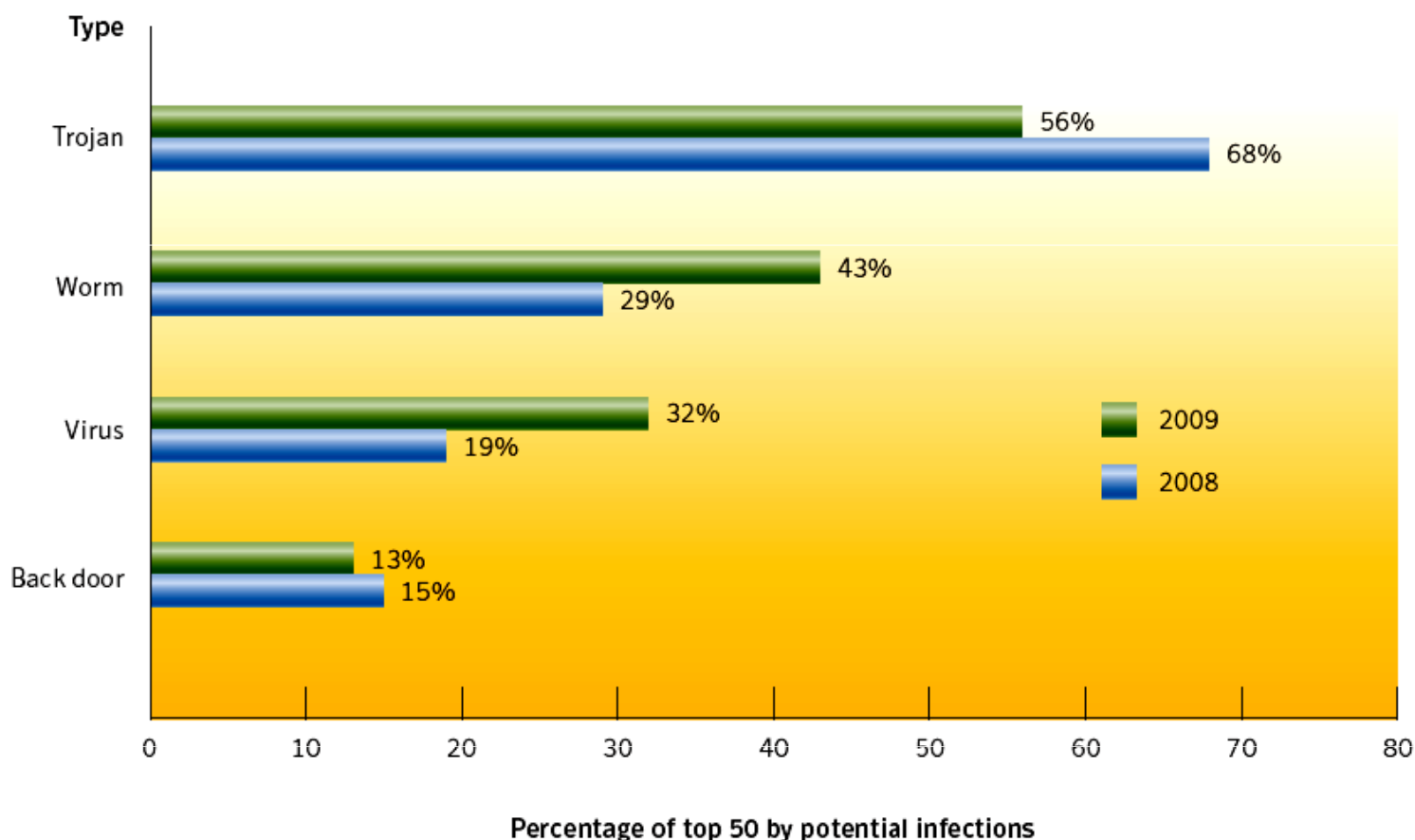


Figure 11. Prevalence of malicious code types by potential infections

Source: Symantec



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world

# Phishing Attacks by Sector

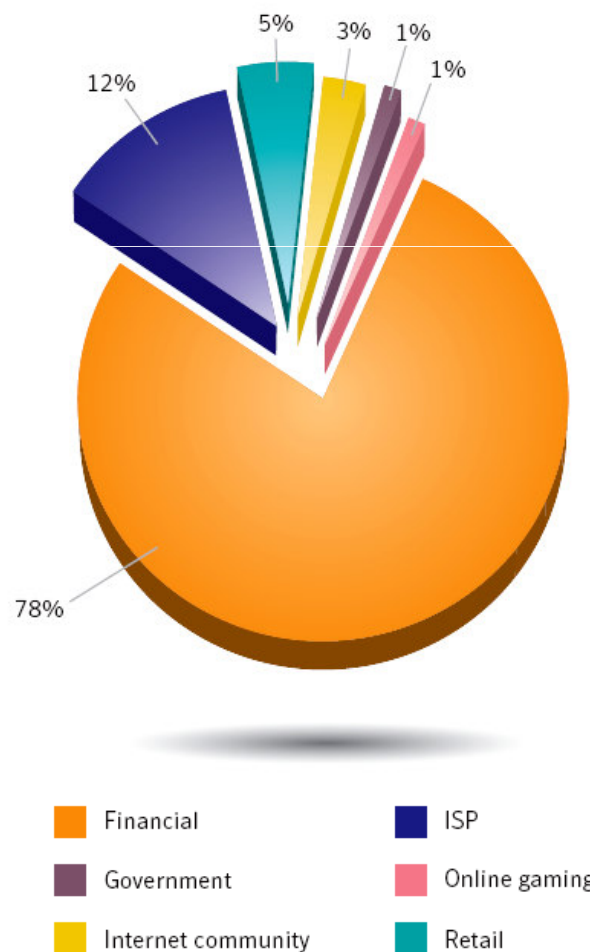


Figure 13. Phished sectors by volume of phishing URLs

Source: Symantec

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



University of Technology,  
Jamaica



Committed to connecting the world

# Threats to Confidential Information

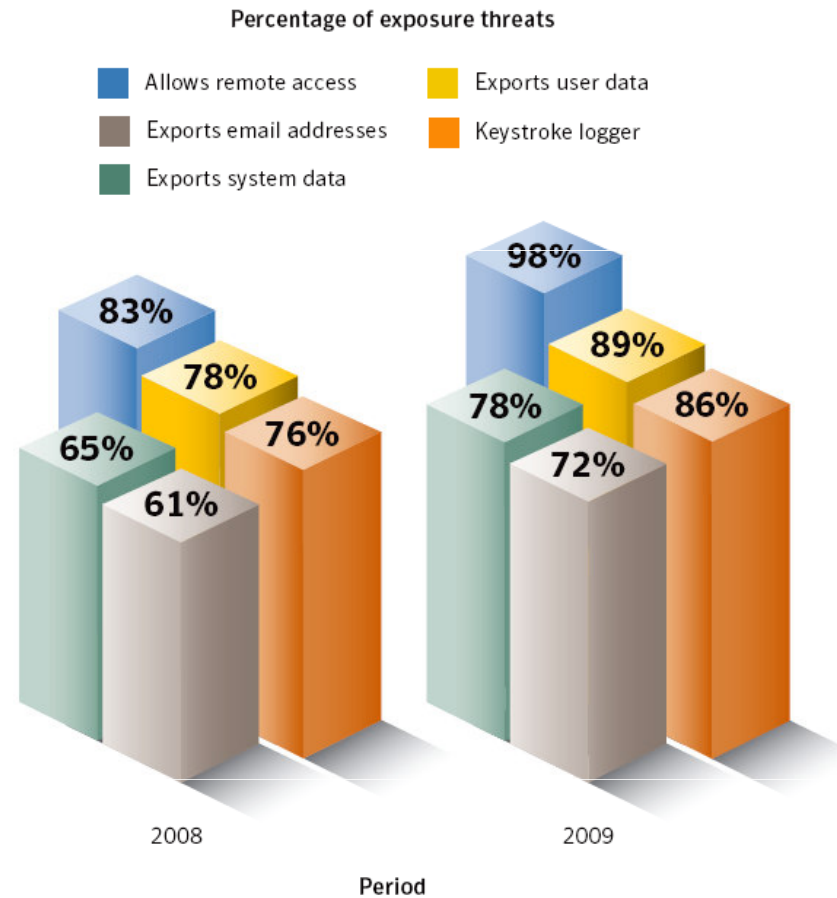


Figure 12. Threats to confidential information, by type

Source: Symantec



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world

# Cybercriminal On-Line Services

Overall Rank 2009 2008		Item	Percentage 2009 2008		Range of Prices
1	1	Credit card information	19%	32%	\$0.85–\$30
2	2	Bank account credentials	19%	19%	\$15–\$850
3	3	Email accounts	7%	5%	\$1–\$20
4	4	Email addresses	7%	5%	\$1.70/MB–\$15/MB
5	9	Shell scripts	6%	3%	\$2–\$5
6	6	Full identities	5%	4%	\$0.70–\$20
7	13	Credit card dumps	5%	2%	\$4–\$150
8	7	Mailers	4%	3%	\$4–\$10
9	8	Cash-out services	4%	3%	\$0–\$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	\$2–\$30

**Table 21. Goods and services advertised for sale on underground economy servers**

Source: Symantec



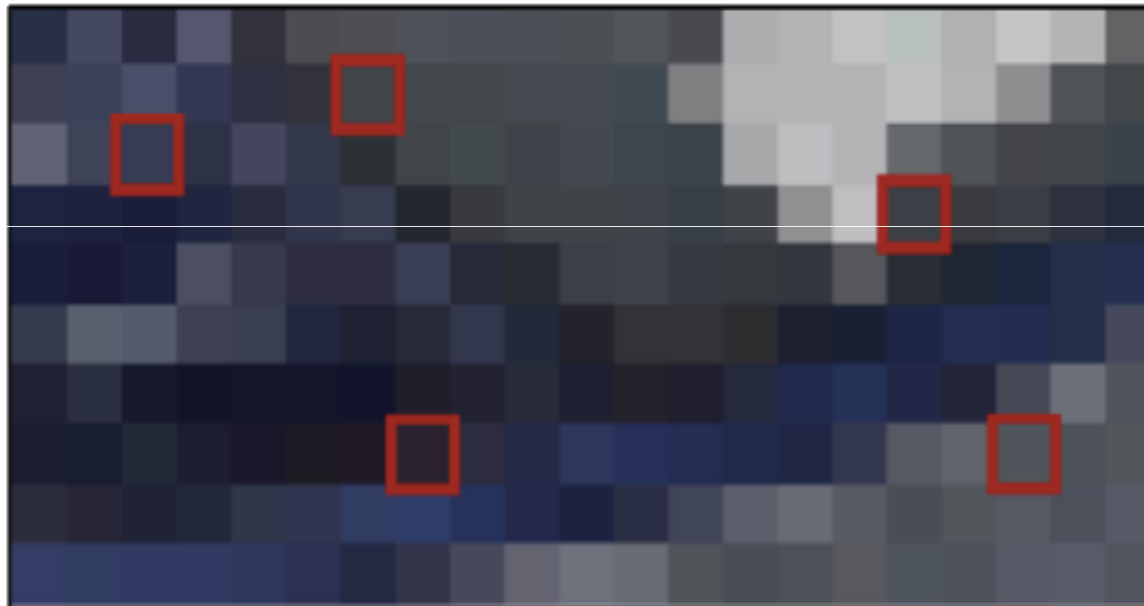
University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world

# Secret Exchange of Criminal Information using Pixel Coding



Graphic 35

The graphic shows how information can be hidden in a picture. The encryption software includes information by altering the colour information of certain pixels. If the picture is sufficiently large, changes can hardly be recognised without having access to the original, as well as the modified, picture. Using this technology, offenders can hide the fact that they are exchanging additional information.



# \* Workshop Session 5 \*

## The Global Cybersecurity Agenda: *...Cybercrime & Legislation*

1 – Definition and Scope	2 – Dimensions of Cybercrime	3 – Cybercrimes against CIIP
4 – National Cybercrime Laws	5 – UK Cyber Legislation	6 – National Cyber Strategies
7 – ITU Cybercrime Toolkit	8 – Digital Forensics	9 – Legislation for Jamaica





# CyberCrimes against Critical Sectors

- *Government:*
  - Theft of secret intelligence, manipulation of documents, and illegal access to confidential citizen databases & national records
- *Banking/Finance:*
  - Denial of Service attacks against clearing bank network, phishing attacks against bank account & credit cards, money laundering
- *Telecomms/Mobile:*
  - Interception of wired & wireless communications, and penetration of secure government & military communications networks
- *Travel/Tourism:*
  - Cyberterrorism against airports, hotels and resorts, malicious penetration of on-line booking & reservations networks
- *Energy/Water:*
  - Manipulation and disruption of the national energy grid & water utilities through interference of the process control network



# \* Workshop Session 5 \*

## The Global Cybersecurity Agenda: *...Cybercrime & Legislation*

1 – Definition and Scope	2 – Dimensions of Cybercrime	3 – Cybercrimes against CIIP
4 – National Cybercrime Laws	5 – UK Cyber Legislation	6 – National Cyber Strategies
7 – ITU Cybercrime Toolkit	8 – Digital Forensics	9 – Legislation for Jamaica



# National Cybercrime Legislation

- **UK :** The UK Government now has a comprehensive set of upgraded laws that provide security in cyberspace
  - We'll discuss these laws & the UK Cyberstrategy as an example of "best practice" for the deployment of cyber legislation & regulations
- **EU:** The Council of Europe established one of the first international treaties to address Computer & Internet Crime
  - We'll discuss the CoE Convention on Cybercrime (CETS No 185)
- **ITU:** The ITU assembled a global team of legal & cybersecurity experts to advise and to develop an in-depth legal toolkit
  - We'll provide an overview and analysis of the ITU Cybercrime Toolkit, and work together today on group tasks related to Cyber Legislation for Jamaica



# Jamaica: Cyber Crimes Act - 2009



Home > Caricom News > JAMAICA- New legislation to deal with cyber crime

## JAMAICA- New legislation to deal with cyber crime

THURSDAY, 18 FEBRUARY 2010 01:01 | CMC

KINGSTON, Jamaica, CMC - Prime Minister Bruce Golding has instructed Attorney General Dorothy Lightbourne to determine the feasibility of new legislation which would make it mandatory for persons buying cellular phones and SIM cards to show identification.



Golding told Parliament on Tuesday that it had become necessary to contemplate a new law in light of the increasing number of crimes being committed by persons using cellular phones.

He said the police have been raising the issue and as a result the authorities were looking at legislative remedies.

"But the intention is subject to legal guidance, either through exercising the authority that we have under the licenses or, if necessary, coming to parliament and asking parliament to enact legislation.

"We are going to have to impose a requirement that when you go to purchase a cell phone or a SIM card you are going to be required to produce your identification which must be recorded," Golding said.

Meanwhile, the House of Representatives has approved the Cyber Crimes Bill, which when enacted, provides law enforcement authorities with greater powers to prosecute persons who hack into computer programmes with criminal intent. Golding, who piloted the bill, said provisions have been made for a special committee to be established to review the cyber crimes law every three years.



# Jamaica Cyber Crimes Act - 2009

## ***Cyber Crime a Serious Problem - PM***

*by Jamaica Information service*

Posted: Feb 12, 2010 19:37 UTC

KINGSTON (JIS) - Prime Minister, Hon. Bruce Golding, says that cyber crime has become a serious problem in Jamaica, which has to be addressed.

"We are particularly familiar with the lotto scam in Montego Bay. It is not just the crime and the fraud that is committed, it is the murder to which it gives rise," Mr. Golding stated as he piloted the Cyber Crimes Act in the House of Representatives on Wednesday (February 10).

The legislation imposes criminal sanctions on the misuse of computer systems or data. Offences covered include: intentional unauthorised access to computer data; access to computer programmes or data with intent to commit any offence; intentional unauthorised modification of a computer programme or data; unauthorised interception of computer function or service; willful unauthorised obstruction of the operation of a computer or denial of access to a computer programme or data; and unlawfully making available, devices or data for the commission of any of the above offences.

The Bill also makes consequential amendments to the Interception of Communications Act, the Mutual Assistance (Criminal Matters) Act, and the Proceeds of Crime Act.

According to the Prime Minister, the legislation is "really just catching up with innovation and technology," which has now become an essential way of life.

He said that more consumers are carrying out business transactions via the Internet and in the United States alone the value of e-commerce sales for 2009 was almost US\$100 billion.



University of Technology,  
Jamaica

**ITU Centres of Excellence Network for the Caribbean Region**  
**Developing a National and Organizational Cybersecurity Strategy**  
13-15 September, Kingston, Jamaica



**Committed to connecting the world**



# Jamaican Cyber Crime Act

## Jamaica passes CyberCrime Bill..



December 20, 2009



Simon Hunt



[Go to comments](#)



[Leave a comment](#)

This week (18th December 2009) Jamaica moved its Cyber Crime bill into law making it possible to prosecute hackers and people who use nefarious popups to collect personal data. The [Jamaica Observer](#) reports-

“ The Bill, which was passed with eight amendments, will see persons convicted of breaches facing a maximum sentence of 10 years’ imprisonment and a minimum of two years; or slapped with fines ranging from between \$2 million and \$5 million.

Previously Jamaica had no definitive legislation for computer related crime, but this new law, The CyberCrime Act of 2009, takes great strides in enabling the efficient prosecution of hackers and IT related criminals.

The Observer highlights the case of 26-year-old computer science student Philpott Martin, who has been hauled before the Courts for allegedly hacking into the system of telecoms giant Digicel and stealing more than \$10 million in calling credit. Martin was charged with three counts of simple larceny and one count of conspiracy to defraud due to the lack of cyber crime legislation under which he could be prosecuted.

This new bill aids in the effective prosecution of eCommerce fraud and Lotto scams, which have become rife in Jamaica due to the lack of effective policy.

eCriminals beware, Jamaica is no longer a safe haven for you!



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world



# Jamaica: Copyright Legislation



## Police Steps Up Anti-Piracy Activities

KINGSTON (JIS):

Wednesday, August 26, 2009

The Jamaica Constabulary Force's (JCF) Organised Crime Investigation Division (OCID) and the Jamaica Intellectual Property Office (JIPO) have teamed to sensitise the public to the implications of breaching Jamaica's copyright laws.

Details were unveiled at a joint media briefing hosted by both agencies, at the Police Officers Club, Hope Road, Kingston, on Tuesday (August 25).

Head of the OCID, Superintendent Fitz Bailey, noted that the initiative comes in light of a seeming unawareness of the dangers which trading in illicit goods, such as bootleg music compact discs (CDs) and movie digital video discs (DVDs), pose for Jamaica in the global context, in addition to threatening the livelihood of the owners of the material.

To this end, he said that both agencies will collaborate on developing a programme targeting these individuals, which they will embark on, shortly. He pointed out that, in light of Jamaica being a signatory to various conventions and treaties on intellectual property, failure by the local authorities to enforce anti-piracy laws, as stipulated by the World Trade Organisation (WTO), would tarnish Jamaica's image, globally.

In disclosing that the police have seized over 50,000 illegal CDs and DVDs, and made some 70 arrests in connection with these activities within the Corporate Area since January, Supt. Bailey underscored their responsibility to ensure that the copyright legislation is enforced.



University of Technology,  
Jamaica

**ITU Centres of Excellence Network for the Caribbean Region**  
**Developing a National and Organizational Cybersecurity Strategy**  
*13-15 September, Kingston, Jamaica*



**Committed to connecting the world**

# Jamaican Intellectual Property Office : JIPO

## Police, JIPO to address copyright breaches

The Jamaica Constabulary Force's (JCF) Organised Crime Investigation Division (OCID) and the Jamaica Intellectual Property Office (JIPO) have teamed to sensitise the public to the implications of breaching Jamaica's copyright laws.

Details were unveiled at a joint media briefing hosted by both agencies, at the Police Officers Club, Hope Road, [Kingston](#), on Tuesday (August 25).

Head of the OCID, Superintendent Fitz Bailey, noted that the initiative comes in light of a seeming unawareness of the dangers which trading in illicit goods, such as bootleg music compact discs (CDs) and movie [digital video discs](#) (DVDs), pose for Jamaica in the global context, in addition to threatening the livelihood of the owners of the material.

To this end, he said that both agencies will collaborate on developing a programme targeting these individuals, which they will embark on, shortly. He pointed out that, in light of Jamaica being a signatory to various conventions and treaties on intellectual property, failure by the local authorities to enforce anti-piracy laws, as stipulated by the World Trade Organisation (WTO), would tarnish Jamaica's image, globally.

### 50,000 illegal CDs and DVDs

In disclosing that the police have seized over 50,000 illegal CDs and DVDs, and made some 70 arrests in connection with these activities within the Corporate Area since January, Supt. Bailey underscored their responsibility to ensure that the copyright legislation is enforced.

"Currently there is a proposal on the table for Copyright legislation, including (the) [Trademark](#) and Patent Act, to be taught at the police training school, so that those (graduates) who are coming fresh out of training will have an appreciation of the legislation, and assist with the enforcement," he outlined.



# \* Workshop Session 5 \*

## The Global Cybersecurity Agenda: *...Cybercrime & Legislation*

1 – Definition and Scope	2 – Dimensions of Cybercrime	3 – Cybercrimes against CIIP
4 – National Cybercrime Laws	5 – UK Cyber Legislation	6 – National Cyber Strategies
7 – ITU Cybercrime Toolkit	8 – Digital Forensics	9 – Legislation for Jamaica



# UK Cybercrime Legislation

UK CYBERCRIME LEGISLATION	
1.	The Official Secrets Acts - 1911 to 1989
2.	The Public Records Acts - 1958 to 1967
3.	The Data Protection Act - 1998
4.	The Freedom of Information Act - 2000
5.	The Human Rights Act - 1998
6.	The Computer Misuse Act 1990
7.	The Copyright Designs and Patents Act 1988
8.	The Civil Evidence Act 1968
9.	The Police and Criminal Evidence Act 1984
10.	The Wireless Telegraphy Act 1949 - 2006
11.	The Communications Act 2003
12.	The Regulation of Investigatory Powers Act 2000 (RIPA)
13.	The Telecommunications Regulations 2000 (Interception)
14.	The Civil Contingencies Act 2004
15.	The Anti-Terrorism, Crime and Security Act 2001
16.	The Forgery and Counterfeiting Act 1981
17.	The Fraud Act 2006
18.	Police Justice Act 2006
19.	The Theft Act - 1978 to 1996
20.	The Cybersecurity Strategy - Cabinet Office - June 2009



# 1. UK Official Secrets Acts 1911 to 1989

## ■ Official Secrets Acts 1911 to 1989

- *Unauthorised Disclosure of Official Information*
- Under the Official Secrets Act 1989, it is an offence for a Crown servant or government contractor to disclose official information in any of the protected categories if the disclosure is made without lawful authority and is damaging to the national interest. It is also an offence if a member of the public, or any other person who is not a Crown servant or government contractor under the Act, has in his or her possession, official information in one of the protected categories, and the information has been disclosed without lawful authority, or entrusted by a Crown servant or government contractor on terms requiring it to be held in confidence.
- *Cybersecurity Relevance: Covers all electronic communications, documents and media whatever format.*



## 2. UK Official Disclosure Public Records Acts 1958 and 1967

### 2. Official Disclosure Public Records Acts 1958 and 1967

- The law on public records is set out in the Public Records Acts of 1958 and 1967. Public records are defined as “administrative and departmental records belonging to Her Majesty’s Government, whether in the United Kingdom or elsewhere”. The Public Records Act of 1958 places a responsibility on all government departments to review the records which are produced within the department, to choose those which are worthy of permanent preservation and transfer them to the Public Records Office (PRO), and to destroy all records which are not selected. The 1967 Act stipulates that all surviving public records should normally be released to the public 30 years after their creation.
- *Cybersecurity Relevance: Now applies to all electronic communications and media*





# 3. UK Data Protection Act 1998

## 3. Data Protection Act 1998

- This Act provides a right of access by living individuals to personal data held about them by any person, subject to any exemption which may apply. It also imposes responsibilities on those who process personal data. The Act requires compliance with eight data protection principles, one of which is ensuring that adequate security is employed when processing personal data.
- The Act also requires those persons who hold personal data to register that fact with the Information Commissioner together with a description of the purpose of processing, data class (the information processed), its sources & the recipients (persons to whom it may be disclosed).
- - *Cybersecurity Relevance: Particularly relevant to all on-line databases, personal information collected by companies, websites, call centres for whatever purposes & in any electronic or physical format*



## 4. UK Freedom of Information Act 2000

### 4. Freedom of Information Act 2000

- The Freedom of Information Act 2000 relates to the publication and disclosure of information held by public authorities. It gives a statutory right of access to information, which entitles any person to be told on request, subject to certain exemptions, whether the Department holds particular information (the duty to confirm or deny) and, assuming that it does, to have that information communicated to them within 20 working days. The Act also requires all public authorities to maintain a Publication Scheme and to release information proactively and keep the scheme under review.
- *Cybersecurity Relevance: Provides the Public with rights to access most on-line personal electronic media*



# 5. UK Human Rights Act 1998

## 5. Human Rights Act 1998

- This Act, which brings the European Convention on Human Rights (ECHR) in UK domestic law, provides every person in the UK certain human rights and fundamental freedoms including the right to privacy and freedom of expression, subject to a number of exceptions. The extent of these rights, including an individual's right to privacy and freedom of expression, has been tested in the European Court of Human Rights and in UK courts by several cases
- - *Cybersecurity Relevance: Provides for personal right to privacy and freedom of expression*



## 6. Communications and Information Systems Computer Misuse Act 1990 – (CMA)

### 6. Communications and Information Systems Computer Misuse Act 1990 – (CMA)

- This deals with the rights of computer owners against the unauthorised use of a computer by any party, making offences of attempted or actual penetration or subversion of computer systems. Under the terms of Section 3 of the Computer Misuse Act it is a criminal offence to introduce unauthorised software into a computer system with the intention of impairing the operation of the computer system or the integrity of any data or program stored within the computer system. Updated through the Police and Justice Act (2006)
- - *Cybersecurity Relevance: This is a key act that makes it illegal to penetrate or hack computer systems, as well as to install malicious codes, "bots", trojans or any other unauthorized software or device.*



# 7. UK Copyright (Computer Programs) Designs & Patents Regulations-1988

## 7. Copyright (Computer Programs) Regulations – Copyright Designs and Patents Act-1988

- Infringement and copying of Computer Software is governed by the Copyright Designs and Patents Act 1988. Individuals and users should be aware that copyright infringements are not exclusively a matter of civil actions for damages by a copyright owner. The criminal penalties for infringing computer software copyright may include heavy fines, imprisonment (for up to 2 years) and the forfeiture of infringing copies and articles for making them. The Director or CEO of an organisation may also be subject to prosecution for permitting the illegal copying of software or its use within the area of their responsibility.
- - *Cybersecurity Relevance: Copying software and other media is relatively easy on-line, but is established as being illegal under the copyright act. Legislation is also applicable for music, videos, DVDs, books and all other forms of copyright or patented materials accessible or downloadable on-line.*



# 8. UK Civil Evidence Act 1968

## 8. Civil Evidence Act 1968

- Provides the basis for the use of computer-based evidence in Civil Proceedings
- - *Cybersecurity Relevance: The prosecution of civil cases may require the collection of electronic materials such as emails, phone records, log files, text messages, & digital photos.*





# 9. UK Police and Criminal Evidence Act 1984

## 9. Police and Criminal Evidence Act 1984

- Provides the basis for the use of computer-based evidence in Criminal Proceedings
- - *Cybersecurity Relevance: The prosecution of criminal cases may require the collection of electronic materials such as emails, phone records, log files, text messages, & digital photos.*



# 10. UK Wireless Telegraphy Act 1949 & 2006

## 10. Wireless Telegraphy Act 1949 and 2006

- This prohibits the unauthorised use of wireless telegraphy apparatus for the transmission or reception and subsequent disclosure of communications.
- - *Cybersecurity Relevance: This act has several applications including it being illegal to penetrate wireless communications networks, and to then use or disclose this information to 3<sup>rd</sup> parties. In principle this could be used in relation to Wi-Fi, Wi-Max networks or any other form of radio, wireless or satellite transmission.*



# 11. UK The Communications Act 2003

## 11. The Communications Act 2003

- This massive integrated Act (over 600 pages) largely repeals the provisions of earlier communications Acts, e.g. Telecommunications Act 1984, and confers functions on the Office of Communications (OFCOM) and makes provision about the regulation of the provision of electronic communications network and services and the use of the electronic spectrum.
- *Cybersecurity Relevance: This is one of the cornerstones of modern UK Legislation relating to electronic communications including the Internet, Broadcast and Telecommunications*



# 12. Regulation of Investigatory Powers Act 2000 (RIPA)

## 12. Regulation of Investigatory Powers Act 2000 (RIPA)

- This is a piece of permissive legislation allowing for the interception of communications, the carrying out of surveillance, and the running of covert human intelligence sources in certain limited circumstances. In relation to the interception of communications, authorisation can only be given by the Secretary of State, and in relation to surveillance and source handling activities authorisation must be given senior official level. The Act also confers on the Secretary of State the power to make orders, regulations or rules under various provisions of the Act. RIPA does not prohibit the interception of communications where all parties have consented to the interception (*see also next slide*).
- *Cybersecurity Relevance: Criminal actions in cyberspace require the investigation of traffic flows, data centres and in-depth surveillance of targeted electronic facilities, infrastructure and assets*



# 13. The Telecommunications (Interception of Communications) Regulations 2000

## 13. The Telecommunications Regulations 2000 (Interception of Communications)

- These Regulations authorise certain interceptions of telecommunication communications which would otherwise be prohibited by section 1 of the Regulation of Investigatory Powers Act 2000. The interception has to be by or with the consent of a person carrying on a business for purposes relevant to that person's business and using that business's own telecommunication system. Interceptions are authorised only if the controller of the telecommunications system on which they are affected has made all reasonable efforts to inform potential users that interceptions may be made.
- *Cybersecurity Relevance: This extends the right for inception & surveillance to collect electronic evidence in the cases that RIPA is not applicable*



# 14. The UK Civil Contingencies Act (2004)

## 14. The Civil Contingencies Act (2004)

- The Civil Contingencies Act, and accompanying non-legislative measures, delivers a single framework for civil protection in the UK. The act is separated into two parts: local arrangements for civil protection (Part1) and emergency powers (Part2). Part 1 of the Act and supporting Regulations and statutory guidance establish a clear set of roles and responsibilities for those involved in emergency preparation and response at the local level. The Act divides local responders into two categories, imposing a difference set of duties on each. Those in Category 1 are those organisations at the core of the response to most emergencies and are subject to the full set of civil protection duties, part of which, is to put in place Business Continuity Management arrangements.
- - *Cybersecurity Relevance: This concerns the responsibilities civil protection, including business continuity planning and disaster recovery in the event of large-scale crisis and emergency for whatever means. Clearly this will involve substantial investment to secure Central Government and Regional cyber infrastructure to ensure no single-points of failure, and to ensure rapid recovery following cyberattacks and on-line threats.*





# 15. The UK Anti-Terrorism, Crime and Security Act 2001

## 15. The Anti-Terrorism, Crime and Security Act 2001

- This relatively recent act includes electronic evidence as well as covering other aspects of 21<sup>st</sup> Century threats, risks and challenges that are closely related to cyberattacks and cybercrime.
- *Cybersecurity Relevance: Establishes the right of the authorities to take away electronic evidence and assets such as laptops, storage & networking device that may then be used as criminal evidence in court.*



# 16. UK Forgery and Counterfeiting Act – 1981

## 16. Forgery and Counterfeiting Act – 1981

- This act covers the forgery of electronic instruments that are accepted as payment in the UK
- - *Cybersecurity Relevance: Cybercrime now frequently uses forged financial accounts, electronic ID Cards and other on-line or off-line coded electronic devices. This act makes forgery of such coded devices illegal.*



# 17. UK Fraud Act 2006

## 17. Fraud Act 2006

- This Act includes any program or data in electronic form as one of the definitions of “article” in terms of possession and use to commit fraud.
- - *Cybersecurity Relevance: Again, there is now cybercrime and on-line fraud that uses electronic programmes, malicious code and other devices to secure illegal financial gain or possession of other assets.*



# 18. UK Police Justice Act 2006

## 18. Police Justice Act 2006

- This is the most recent amendment of the Computer Misuse Act (CMA)
- - *Cybersecurity Relevance: Legislation needs to be continuously reviewed and updated to make sure that it covers the latest criminal opportunities provided by technological & scientific developments.*



# 19. UK Theft Act 1978 to 1996

## 19. Theft Act 1978 to 1996

- The Theft Act covers the theft of services, monetary instruments or credit.
- *Cybersecurity Relevance: Increasingly cybercrime is targeting non-physical financial & electronic assets and services, so the definition of theft is extended to include such crime in cyberspace.*



## 20. Cybersecurity Strategy of the United Kingdom – 2009

### 20. Cybersecurity Strategy of the United Kingdom – June 2009

- Although this document is not itself a Law nor Regulation, it will still be of significant value to the Georgian Government since it provides one of the most recent comprehensive national cybersecurity strategies that is driven through the UK Office of Cybersecurity within the Cabinet Office. We would also recommend that the Georgian Government also reviews the Cybersecurity Policy Review to President Obama (June 2009) – “Assuring a Trusted and Resilient Information and Communications Infrastructure”.
- *Cybersecurity Relevance: Every country now requires a cohesive national strategy to secure its borders in cyberspace, and the UK Strategy Document is an excellent template to study as the basis for a possible Jamaican National Cybersecurity Agency.*



# \* Workshop Session 5 \*

## The Global Cybersecurity Agenda: *...Cybercrime & Legislation*

1 – Definition and Scope	2 – Dimensions of Cybercrime	3 – Cybercrimes against CIIP
4 – National Cybercrime Laws	5 – UK Cyber Legislation	6 – National Cyber Strategies
7 – ITU Cybercrime Toolkit	8 – National Cybercrime Unit	9 – Legislation for Jamaica



# European Convention on Cybercrime - 2001

- **CoE** : The UK Laws summarised during this 3-day workshop provide an excellent template for Jamaica to review its own cybersecurity Legislation. It is also recommended to fully understand the provisions of the Council of Europe (CoE) Cybercrime Convention (CETS 185)
- **EU Legislation**: Topics that need to be considered include: i) Illegal Access , ii) Illegal Interception, iii) Data Interference, iv) System Interference, v) Illegal Devices, vi) Computer Sabotage, vii) Child Pornography viii) IPR & Copyright Laws ix) Computer System Search and Evidence, x) Computer Fraud, and xi) Jurisdiction. The full CoE Cybercrime Convention will be found on-line at: [www.coe.int/cybercrime/](http://www.coe.int/cybercrime/)

....*The Convention on Cybercrime has been signed by more than 45 countries (including Canada, Japan, South Africa and USA), and ratified by 29 countries (including USA)*



# UK Government Cybersecurity Strategy–June 2009

- ❑ UK Cabinet Office published National Cyberstrategy – 2009
- ❑ Established Cross-Government Programme to address Priorities
- ❑ Set up OCS : Office of Cybersecurity
- ❑ Created CSOC : Cybersecurity Operations Centre (CSOC)
- ❑ Available for online download at: [www.cabinetoffice.gov.uk](http://www.cabinetoffice.gov.uk)

To address the UK's cyber security challenges, the Government will:

- **Establish a cross-government programme**, with additional funding to address the following priority areas in pursuit of the UK's strategic cyber security objectives:
  - Safe Secure & Resilient Systems
  - Policy, Doctrine, Legal & Regulatory issues
  - Awareness & Culture Change
  - Skills & Education
  - Technical Capabilities & Research and Development
  - Exploitation
  - International Engagement
  - Governance, Roles & Responsibilities
- **Work closely with** the wider public sector, industry, civil liberties groups, the public and with international partners;
- **Set up an Office of Cyber Security (OCS)** to provide strategic leadership for and coherence across Government;
- **Create a Cyber Security Operations Centre (CSOC)** to:
  - actively monitor the health of cyber space and co-ordinate incident response;
  - enable better understanding of attacks against UK networks and users;
  - provide better advice and information about the risk to business and the public.



# \* Workshop Session 5 \*

## The Global Cybersecurity Agenda: *...Cybercrime & Legislation*

1 – Definition and Scope	2 – Dimensions of Cybercrime	3 – Cybercrimes against CIIP
4 – National Cybercrime Laws	5 – UK Cyber Legislation	6 – National Cyber Strategies
7 – ITU Cybercrime Toolkit	8 – Digital Forensics	9 – Legislation for Jamaica



# ITU Toolkits: Cybercrime Legislation and a Cybercrime Guide for Developing Countries

International Telecommunication Union  
Cybercrime Legislation Resources



## ITU TOOLKIT FOR CYBERCRIME LEGISLATION

Developed through the  
American Bar Association's Privacy & Computer Crime Committee  
Section of Science & Technology Law  
With Global Participation

ICT Applications and Cybersecurity Division  
Policies and Strategies Department  
ITU Telecommunication Development Sector

Draft Rev. February 2010

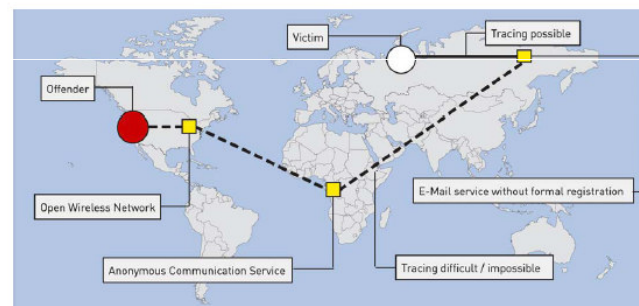
For further information, please contact the  
ITU-D ICT Applications and Cybersecurity Division at [cybmail@itu.int](mailto:cybmail@itu.int)



University of Technology,  
Jamaica

**ITU Centres of Excellence Network for the Caribbean Region**  
**Developing a National and Organizational Cybersecurity Strategy**  
*13-15 September, Kingston, Jamaica*

International Telecommunication Union  
Cybercrime Legislation Resources



## UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES

ICT Applications and Cybersecurity Division  
Policies and Strategies Department  
ITU Telecommunication Development Sector

Draft April 2009

For further information, please contact the  
ITU-D ICT Applications and Cybersecurity Division at [cybmail@itu.int](mailto:cybmail@itu.int)



**Committed to connecting the world**

# ITU Cybercrime Toolkit – Feb 2010

- *ITU Toolkit:* An excellent toolkit for countries such as Jamaica to review and update legislation to reflect all aspects of cybercrime & cyberterrorism. Successive sections of the ITU toolkit consider:
- *Substantive Provisions:* Acts Against Computers, Computer Systems, Networks, Computer Data, Content Data, and Traffic Data
- *Procedural Provisions:* for Criminal Investigations and Proceedings for Offenses Within this Law
- *Jurisdictional Provisions* and International Cooperation
- *Country Work Sheets:* In-Depth Templates that comprehensively span most of the conceivable cybercrime activities & attacks that may occur
- *International Comparisons:* Matrix of Provisions of the Cybercrime Laws that were reviewed from major countries as the basis for the toolkit





## ITU CYBERCRIME TOOLKIT LEGISLATIVE REQUIREMENTS

### Acts Against Computers, Computer Systems, Networks, Computer Data, Content Data, and Traffic Data

Section 1: Definition of Terms

Section 2: Unauthorized Access to Computers, Computer Systems, and Networks

Section 3: Unauthorized Access to or Acquisition of Computer Data, Content Data, Traffic Data

Section 4: Interference and Disruption

Section 5: Interception

Section 6: Misuse and Malware

Section 7: Digital Forgery

Section 8: Digital Fraud, Procure Economic Benefit

Section 9: Extortion

Section 10: Aiding, Abetting, and Attempting

Section 11: Corporate Liability

### Provisions for Criminal Investigations and Proceedings for Offenses within this Law

Section 12: Scope of Procedural Provisions

Section 13: Conditions and Safeguards

Section 15: Expedited Preservation and Partial Disclosure of Traffic Data

Section 17: Production Order

Section 18: Search and Seizure of Stored Data

Section 19: Interception (Real Time Collection) of Traffic Data

Section 20: Interception (Real Time Collection) of Content Data

### Jurisdictional Provisions

Section 21: Jurisdiction

### International Cooperation

Section 22: International Cooperation: General Principles

Section 23: Extradition Principles

Section 24: Mutual Assistance: General Principles

Section 25: Unsolicited Information

Section 26: Procedures for Mutual Assistance

Section 27: Expedited Preservation of Stored Computer Data, Content Data, or Traffic Data

Section 28: Expedited Disclosure of Preserved Content Data, Computer Data or Traffic

Section 29: Mutual Assistance Regarding Access to Stored Computer Data, Content Data, or Traffic Data

Section 30: Trans Border Access to Stored Computer Data, Content Data, or Traffic Data

Section 31: Mutual Assistance In Real Time Collection of Traffic Data

Section 32: Mutual Assistance Regarding Interception of Content Data or Computer Data



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world

# ITU TOOLKIT FOR CYBERCRIME LEGISLATION – COUNTRY WORK SHEET (1) -

Provision in sample language	In local law?	Citation of provision	Consistent with Toolkit?	Needs to be amended?	Needs to be deleted?	Needs to be added?	Comments (reason for amendment or deletion)
<i>Preamble</i>							
<i>Definitions</i>							
<i>a. Access</i>							
<i>b. Computer</i>							
<i>c. Computer Data</i>							
<i>d. Computer Program</i>							
<i>e. Computer System</i>							
<i>f. Content Data</i>							
<i>g. Critical Infrastructure</i>							
<i>h. Cyberspace</i>							



# ITU TOOLKIT FOR CYBERCRIME LEGISLATION

## – COUNTRY WORK SHEET (2) –

Provision in sample language	In local law?	Citation of provision	Consistent with Toolkit?	Needs to be amended?	Needs to be deleted?	Needs to be added?	Comments (reason for amendment or deletion)
i. <i>Damage</i>							
j. <i>Disruption</i>							
k. <i>Interception</i>							
l. <i>Interference</i>							
m. <i>Loss</i>							
n. <i>Malware</i>							
o. <i>Network</i>							
p. <i>Service Provider</i>							
q. <i>Subscriber Information</i>							
r. <i>Traffic Data</i>							
<b>SUBSTANTIVE PROVISIONS</b>							
2. <i>Unauthorized Access to Computers, Computer Systems, and Networks</i>							
a. <i>Unauthorized Access to Computers, Computer Systems, and Networks</i>							
b. <i>Unauthorized Access to Gov't Computers, Computer Systems</i>							



# ITU TOOLKIT FOR CYBERCRIME LEGISLATION

## – COUNTRY WORK SHEET (3) –

Provision in sample language	In local law?	Citation of provision	Consistent with Toolkit?	Needs to be amended?	Needs to be deleted?	Needs to be added?	Comments (reason for amendment or deletion)
<i>and Networks</i>							
<i>c. Unauthorized Access to Critical Infrastructure</i>							
<i>d. Unauthorized Access for Purposes of Terrorism</i>							
<i>3. Unauthorized Access to Computer Program, Computer Data, Content Data, Traffic Data</i>							
<i>a. Unauthorized Access of Computer Program, Computer Data, Content Data, Traffic Data</i>							
<i>b. Unauthorized Access to Protected Government Computer Program or Data</i>							
<i>c. Unauthorized Access to Government Computer Program or Data</i>							
<i>d. Unauthorized Access to Critical Infrastructure Program or Data</i>							



# Matrix of Provision of Cybercrime Laws (1)

Legal Provision	CoE	Australia	Canada	EU	Germany	Japan	Mexico	Singapore	UK <sup>29</sup>	US	India	China
Illegal Interception	X	X <sup>54</sup>	X <sup>55</sup>		X <sup>56</sup>		X	X <sup>57</sup>	X <sup>58</sup>	X <sup>59</sup>	X <sup>60</sup>	X <sup>61</sup>
Data Interference	X	X <sup>62</sup>	X <sup>63</sup>	X	X <sup>64</sup>	X <sup>65</sup>	X	X <sup>66</sup>	X	X	X <sup>67</sup>	X <sup>68</sup>
System Interference	X	X <sup>69</sup>	X <sup>70</sup>	X	X <sup>71</sup>	X	X	X <sup>72</sup>	X		X <sup>73</sup>	X <sup>74</sup>
Misuse of Devices	X	X	X <sup>75</sup>	X		?		X <sup>76</sup>	X	X <sup>77</sup>	X <sup>78</sup>	
Computer-related Forgery	X		X <sup>79</sup>	X	X <sup>80</sup>	X		X <sup>81</sup>	X	X <sup>82</sup>	X <sup>83</sup>	X <sup>84</sup>

Legal Provision	CoE	Australia	Canada	EU	Germany	Japan	Mexico	Singapore	UK <sup>29</sup>	US	India	China
Computer-related Fraud	X		X <sup>85</sup>		X <sup>86</sup>	X		X <sup>87</sup>	X	X <sup>88</sup>	X <sup>89</sup>	X <sup>90</sup>
Offences Related to Child Pornography	X		X <sup>91</sup>	X	X <sup>92</sup>	X?	X	X <sup>93</sup>	X	X <sup>94</sup>	X <sup>95</sup>	X <sup>96</sup>
Offenses Related to Infringements of Copyright And Related Rights	X		X <sup>97</sup>	X	X <sup>98</sup>	X <sup>99</sup>	X	X <sup>100</sup>	X	X		X <sup>101</sup>
Attempt and Aiding	X		X <sup>102</sup>	X	X <sup>103</sup>	X <sup>104</sup>		X <sup>105</sup>	X	X <sup>106</sup>	X <sup>107</sup>	X <sup>108</sup>

# Matrix of Provision of Cybercrime Laws (2)

Legal Provision	CoE	Australia	Canada	EU	Germany	Japan	Mexico	Singapore	UK <sup>29</sup>	US	India	China
And Abetting												
Corporate Liability	X		X <sup>109</sup>	X	X <sup>110</sup>						X <sup>111</sup>	X <sup>112</sup>
Sanctions and Measures	X	X <sup>113</sup>	X	X	X <sup>114</sup>			X <sup>115</sup>	X		X <sup>116</sup>	X <sup>117</sup>
<b>Procedural Law</b>							X					
Scope of Procedural Provisions	X		X <sup>118</sup>	X						X		
Conditions and Safeguards	X	X	X <sup>119</sup>	X				X <sup>120</sup>	X <sup>121</sup>	X		
Expedited Preservation of Stored Computer Data	X	X	X <sup>122</sup>	X	X <sup>123</sup>					X		
Expedited Preservation and	X			X	X <sup>124</sup>					X		X <sup>125</sup>



# Matrix of Provision of Cybercrime Laws (3)

Legal Provision	CoE	Australia	Canada	EU	Germany	Japan	Mexico	Singapore	UK <sup>29</sup>	US	India	China
Partial Disclosure of Traffic Data												
Production Order	X		X <sup>126</sup>	X	X <sup>127</sup>			X <sup>128</sup>	X	X		
Search & Seizure of Stored Computer Data	X	X	X <sup>129</sup>	X	X <sup>130</sup>			X <sup>131</sup>		X	X <sup>132</sup>	X <sup>133</sup>
Real-time Collection of Traffic Data	X		X <sup>134</sup>	X	X <sup>135</sup>				X	X		X <sup>136</sup>
Interception of Content Data	X	X	X <sup>137</sup>	X	X <sup>138</sup>				X	X		X <sup>139</sup>
<b>Jurisdiction</b>												
Jurisdiction	X		X <sup>140</sup>	X	X <sup>141</sup>			X <sup>142</sup>	X			X <sup>143</sup>



# Matrix of Provision of Cybercrime Laws (4)

Legal Provision	CoE	Australia	Canada	EU	Germany	Japan	Mexico	Singapore	UK <sup>29</sup>	US	India	China
International Cooperation			X <sup>144</sup>									
General Principles Relating To International Cooperation	X			X					X			
Extradition	X			X	X <sup>145</sup>	X <sup>146</sup>	X		X			X <sup>147</sup>
General Principles Relating To Mutual Assistance	X			X	X <sup>148</sup>	X?			X			
Spontaneous Information	X			X	X <sup>149</sup>							
Procedures Pertaining to Mutual Assistance Requests In the Absence of Applicable International Agreements	X			X	X <sup>150</sup>				X			
Confidentiality & Limitation On Use	X			X	X <sup>151</sup>				X			
Expedited Preservation of	X			X	X <sup>152</sup>							

# Matrix of Provision of Cybercrime Laws (5)

Legal Provision	CoE	Australia	Canada	EU	Germany	Japan	Mexico	Singapore	UK <sup>29</sup>	US	India	China
Stored Computer Data												
Expedited Disclosure of Preserved Traffic Data	X			X	X <sup>153</sup>							
Mutual Assistance Regarding Accessing of Stored Computer Data	X			X	X <sup>154</sup>							
Trans-border Access to Stored Computer Data With Consent on Where Publicly Available	X			X	X <sup>155</sup>							
Mutual Assistance in the Real-Time Collection of Traffic Data	X			X	X <sup>156</sup>				X			
Mutual Assistance Regarding The Interception of Content Data	X			X	X <sup>157</sup>				X			
24/7 Network	X			X	X <sup>158</sup>							



# \* Workshop Session 5 \*

## The Global Cybersecurity Agenda: *...Cybercrime & Legislation*

1 – Definition and Scope	2 – Dimensions of Cybercrime	3 – Cybercrimes against CIIP
4 – National Cybercrime Laws	5 – UK Cyber Legislation	6 – National Cyber Strategies
7 – ITU Cybercrime Toolkit	8 – Digital Forensics	9 – Legislation for Jamaica



# Legislation to support Digital Evidence & Forensics for Cybercrime Investigations

- **Laws:** Require supporting legislation to permit the collection, processing & analysis of digital evidence as the basis for civil & criminal prosecutions:
  - Mobile Phones, Wi-Fi Devices & Multi-Media Gadgets :
  - Legal interception of network communication:
  - Analysis of storage & memory devices:
  - Access to encrypted data streams & servers:
  - Securing, seizing and transporting equipment from search scenes
  - Professional Training of Evidence Recovery Staff
  - Provision of Audit Trail for all Electronic Investigation Processes
- **"A Good Practice Guide for Computer-Based Electronic Evidence":** Booklet written for ACPO – Association of Chief Police Officers (UK) for the Police Central e-crime Unit available for download: [www.met.police.uk/pceu/](http://www.met.police.uk/pceu/)



# **\* Workshop Session 5 \***

## **The Global Cybersecurity Agenda: ...Cybercrime & Legislation**

<b>1 – Definition and Scope</b>	<b>2 – Dimensions of Cybercrime</b>	<b>3 – Cybercrimes against CIIP</b>
<b>4 – National Cybercrime Laws</b>	<b>5 – UK Cyber Legislation</b>	<b>6 – National Cyber Strategies</b>
<b>7 – ITU Cybercrime Toolkit</b>	<b>8 – Digital Forensics</b>	<b>9 – Legislation for Jamaica</b>





# Jamaica: Practical Agenda to deter Cybercrime

Based upon the ITU Cybercrime Toolkit Methodology we suggest:

- **New Laws:** Enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime consistent with, among others, the provisions of the European Convention on Cybercrime (2001)
- **Legal Authorities:** Assess the current legal authorities for adequacy. Jamaica should review its existing criminal code to determine if it is adequate to address current (and future) problems
- **Cybercrime:** Draft and adopt substantive, procedural and mutual assistance laws and policies to address computer-related crime:
- **E-Crime Unit:** Establish or identify national cybercrime units:
- **PPP – Public and Private Partnerships:** Develop relationships with the national cybersecurity infrastructure and private sector:
- **Professional Legal Awareness:** Develop an understanding among Prosecutors, Judges, and Legislators of Cybercrime Issues
- **24/7 Cybercrime Point:** Propose Jamaican Participation in the International 24/7 Cybercrime Contact Point Network



# Next Steps: Cybersecurity Legislation for Jamaica

We suggest the following steps as the way forward for Jamaica:

- 1) Initiate Programme within the Government Cabinet Office
- 2) Appoint Top-Level Cybersecurity Legislation Team
- 3) Establish National Cybersecurity Agency (NCA)
- 4) Review all existing Legislation & Regulations
- 5) Launch High-Tech Cybercrime Investigation Unit
- 6) Establish 24/7 Contact Point for International Cybercrime
- 7) Draft New Laws & Upgrade existing Legislation & Regulations
- 8) Parliament & Government Cybersecurity Legal Review
- 9) Adoption and Implementation of Legislation



# \* ITU Cybersecurity Strategy \*

## *"3-Day Workshop Overview"*

<b>S1- Mon: 9:30-11:00</b>  <b>"The Cybersecurity Challenge!..."</b>	<b>S2-Mon: 11:30-13:00</b>  <b>"The Need for Action!"</b>	<b>S3 - Mon:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Cybersecurity Action Plans"</b>	<b>S4 - Mon:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Cybersecurity Action Plans"</b>
<b>S5- Tues: 9:30-11:00</b>  <b>ITU Cyber Agenda: 1</b> <b>"Cybercrime and Legislation"</b>	<b>S6-Tues: 11:30-13:00</b>  <b>ITU Cyber Agenda: 2</b> <b>"Technological Risks and Solutions"</b>	<b>S7 -Tues:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Legislation and Regulations"</b>	<b>S8 -Tues:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Legislation and Regulations"</b>
<b>S9- Wed: 9:30-11:00</b>  <b>ITU Cyber Agenda: 3</b> <b>"Operational Risks and Organisational Structures"</b>	<b>S10-Wed:11:30-13:00</b>  <b>ITU Cyber Agenda: 4&amp;5</b> <b>"Capacity Building and Collaboration"</b>	<b>S11-Wed:14:00-15:30</b> <b>Group Session:</b>  <b>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</b>	<b>S12-Wed:16:00-17:30</b> <b>Group Session:</b>  <b>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</b>



# \* Workshop Session 6 \*

## ITU Global Cybersecurity Agenda: ...*Technological Risks & Solutions*

<b>1 – Technologies &amp; Standards</b>	<b>2 – Sources of Cyber Threats</b>	<b>3 – Risk Assessment Model</b>
<b>4 – Risk Assessment &amp; Audit</b>	<b>5 – Cybersecurity Technologies</b>	<b>6 – Physical Security</b>
<b>7 – Business Continuity</b>	<b>8 – ICT Infrastructure Tools</b>	<b>9 – ICT Implementation Plans</b>



# \* Workshop Session 6 \*

## ITU Global Cybersecurity Agenda: ...*Technological Risks & Solutions*

<b>1 – Technologies &amp; Standards</b>	<b>2 – Sources of Cyber Threats</b>	<b>3 – Risk Assessment Model</b>
<b>4 – Risk Assessment &amp; Audit</b>	<b>5 – Cybersecurity Technologies</b>	<b>6 – Physical Security</b>
<b>7 – Business Continuity</b>	<b>8 – ICT Infrastructure Tools</b>	<b>9 – ICT Implementation Plans</b>



# Cyber Technologies and Standards

- *Architectures & Standards:* The protection of critical national infrastructure requires systems & services to be implemented to internationally agreed architectures & technical standards
- *ITU Standards:* Standards Groups supported by the ITU have defined and published an extensive set of standards based around X.805 and X.1205b that cover practically all aspect of cybersecurity systems
- *Integrated Security:* The implementation of complete cybersecurity security solutions for critical sectors requires the integration of cybersecurity technologies within those for physical security
- *Open Wireless World:* The open world of mobile gadgets & social networking means that cybersecurity professionals have to continually design new technical solutions to maintain comprehensive security





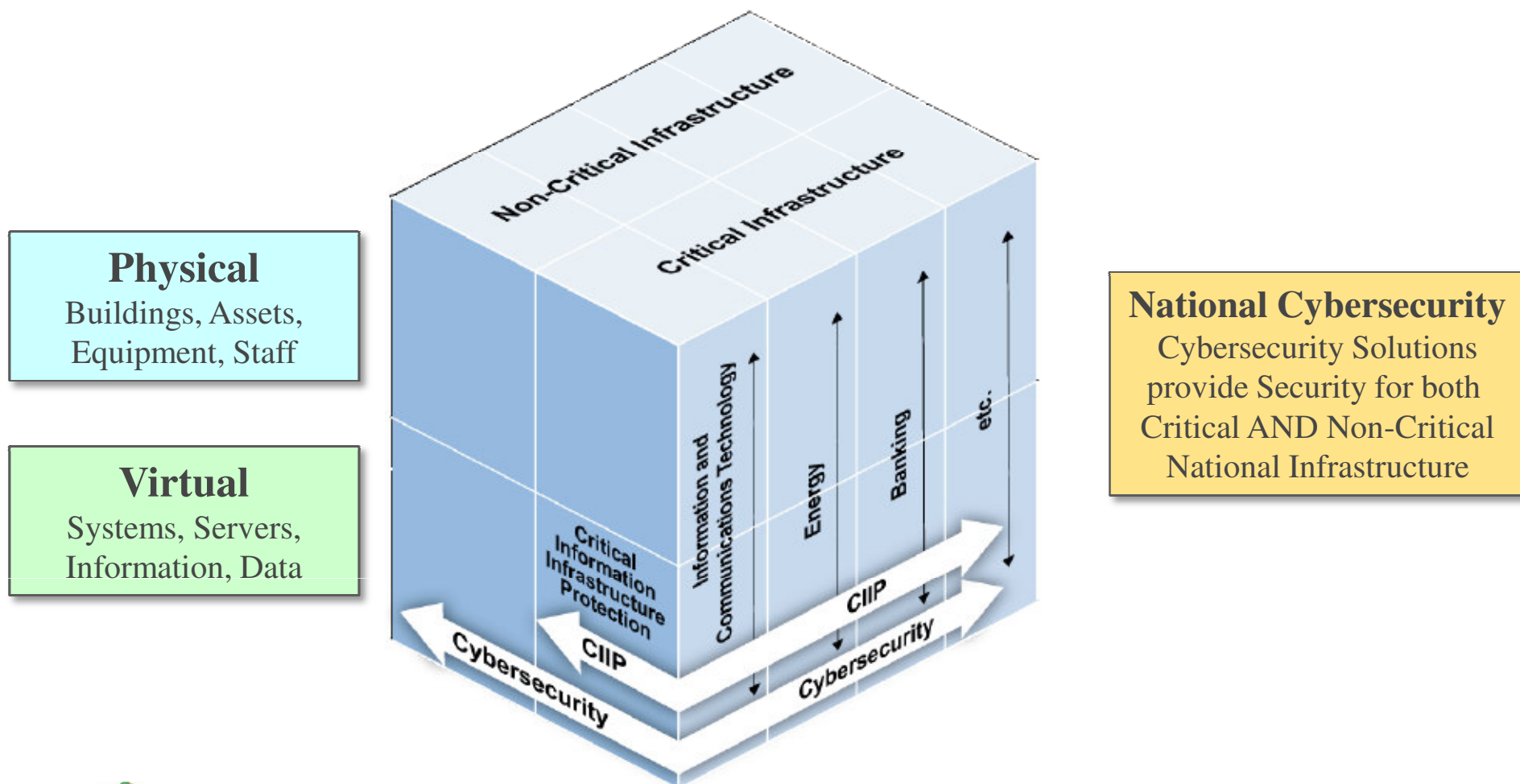
# Definition of Cybersecurity from ITU Technical Standard X.1205

- *“the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, users, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity ensures the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment. The security properties include one or more of the following: availability; integrity (which may include authenticity and non-repudiation); confidentiality” ....*

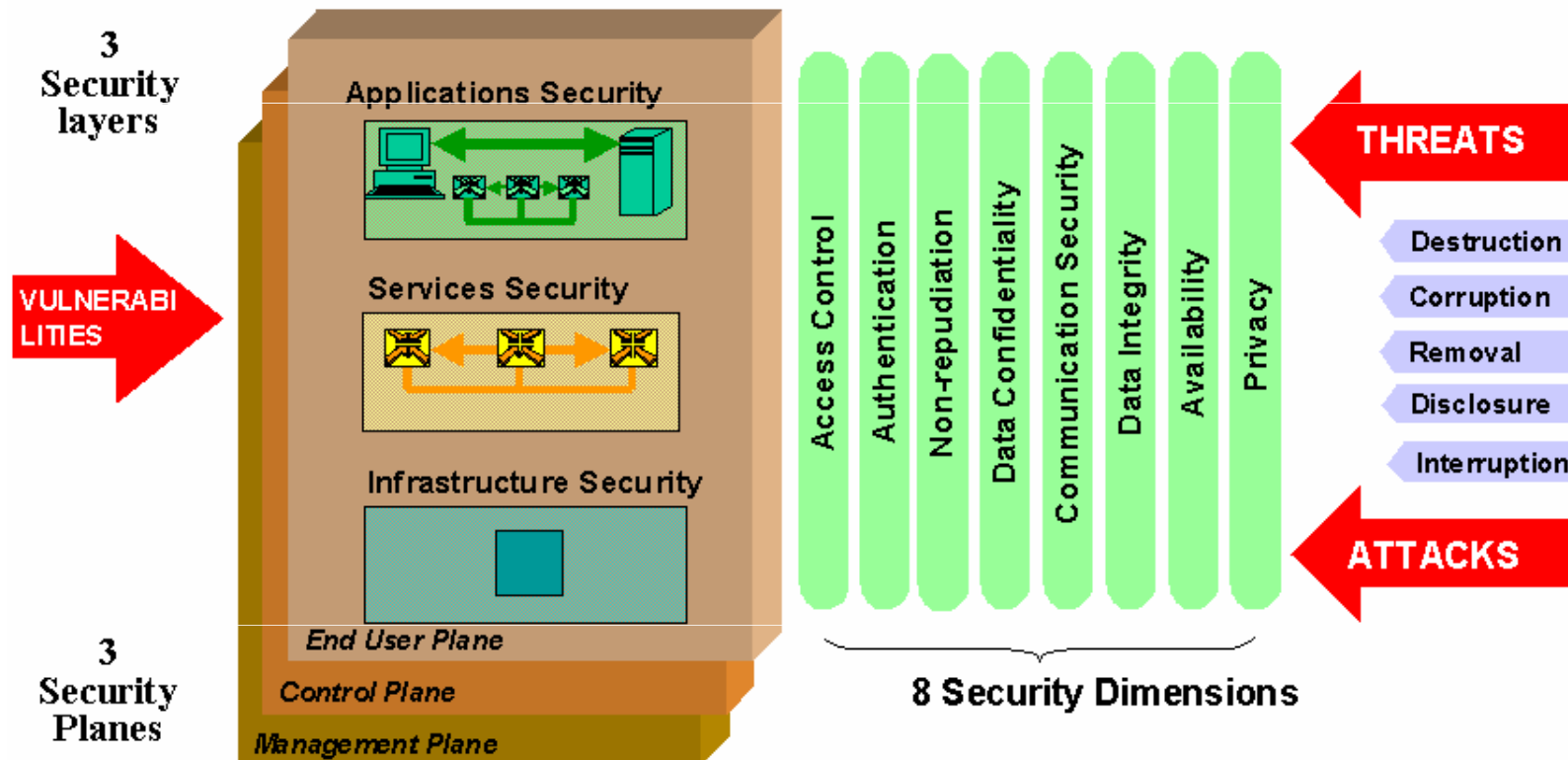
*.....But what does this mean in practice?*



# Security Framework for National Infrastructure Protection



# ITU – X.805 Security Architecture



# \* Workshop Session 6 \*

## ITU Global Cybersecurity Agenda: ...*Technological Risks & Solutions*

1 – Technologies & Standards	2 – Sources of Cyber Threats	3 – Risk Assessment Model
4 – Risk Assessment & Audit	5 – Cybersecurity Technologies	6 – Physical Security
7 – Business Continuity	8 – ICT Infrastructure Tools	9 – ICT Implementation Plans



# Sources of Cyber Threats

- The complexity of cyber threats means that several complimentary frameworks have been developed that classify the risks:
- For this session we'll focus on the categorisation developed by the ITU Telecommunications Study Group 17 as follows:

*Category 1 : **Unauthorised Access** – The systems & networks are accessed by persons or "bots" that do not have legal access or permissions*

*Category 2 : **Denial of Service Attacks (DoS)** – Such attacks are used to target & disable a specific website or server using an army of infected machines*

*Category 3 : **Malicious Code** – Malware such as trojans, viruses & spyware are embedded within host machines for both commercial & criminal purposes*

*Category 4 : **Improper Use of Systems** – In these cases, the systems are being used for access and applications against the communicated policies*

*Category 5 : **Unauthorised Access AND Exploitation** – Many attacks will fall into this category when the hacker will penetrate systems and then use the acquired data, information & documents for cybercriminal activities*

*Category 6 : **Other Unconfirmed Incidents** – These are alerts that require further investigation to understand whether they are actually malicious*



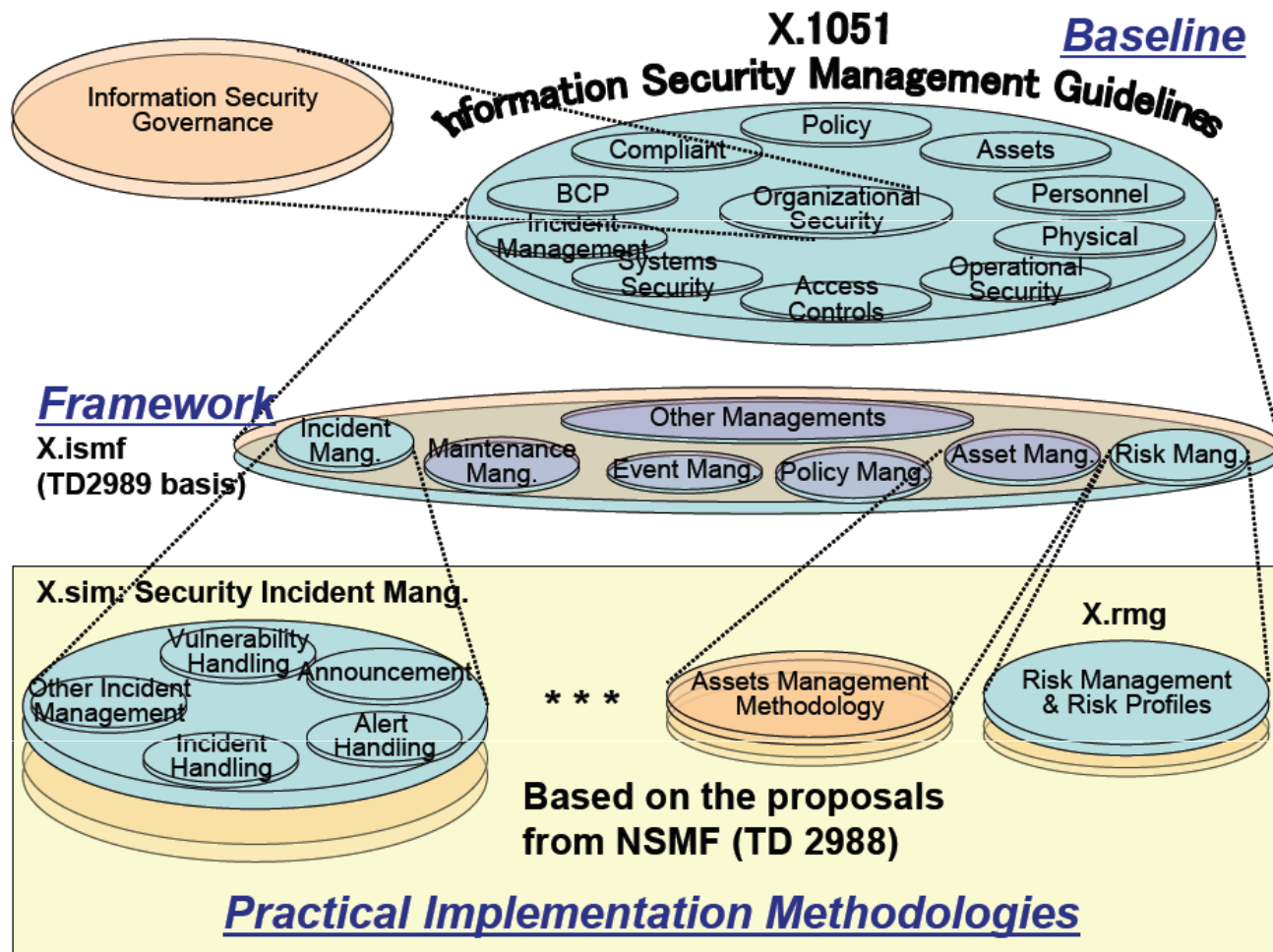
# Cyber Threat Sources against Critical National Infrastructure

# Item	THREAT SOURCE NAME	THREAT LEVEL
1	Foreign Intelligence Agencies	Severe
2	Hackers (Individual & National Hackers)	Severe
3	Organised Crime	Severe
4	Unreliable Employees	Moderate
5	Infrastructure Owners and Operators	Moderate
6	Political Activists	Low
7	Investigative Journalists	Negligible





# Categorisation of Cyber Threats based upon the Information Security Management Guidelines



# \* Workshop Session 6 \*

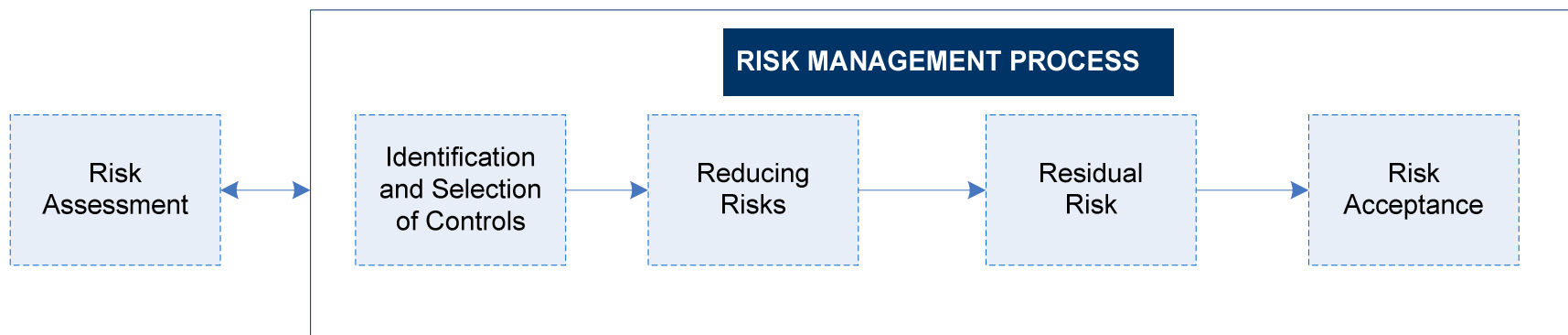
## ITU Global Cybersecurity Agenda: ...*Technological Risks & Solutions*

1 – Technologies & Standards	2 – Sources of Cyber Threats	3 – Risk Assessment Model
4 – Risk Assessment & Audit	5 – Cybersecurity Technologies	6 – Physical Security
7 – Business Continuity	8 – ICT Infrastructure Tools	9 – ICT Implementation Plans

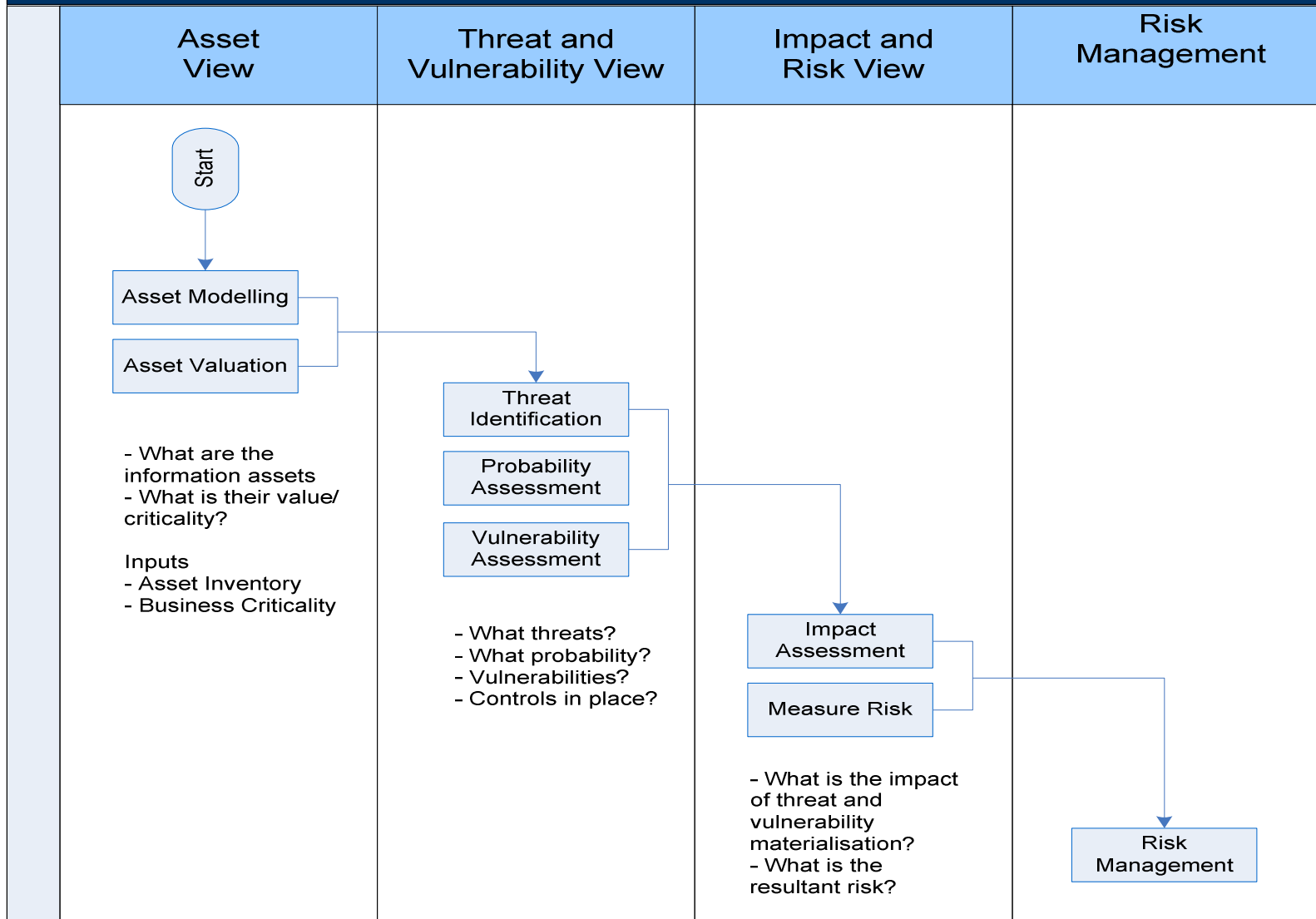


# Cyber Risk Assessment Model

- Cyber threats & attacks need to be assessed within a framework
- The appropriate model that we'll be exploring later in the workshop is that of the CERT or CSIRT – Computer Emergency Response Team
- The typical operational process that will be followed by a CERT:
  - 1) Identification of the cyber risks
  - 2) Analysis, categorisation, and in-depth evaluation the risks
  - 3) Identification of the alternative options for the management of risks
  - 4) Selection of control objectives for the treatment & mitigation of risks



# RISK ASSESSMENT MODEL



## Risk Assessment Flow Chart



# **\* Workshop Session 6 \***

## **ITU Global Cybersecurity Agenda: ...*Technological Risks & Solutions***

<b>1 – Technologies &amp; Standards</b>	<b>2 – Sources of Cyber Threats</b>	<b>3 – Risk Assessment Model</b>
<b>4 – Risk Assessment &amp; Audit</b>	<b>5 – Cybersecurity Technologies</b>	<b>6 – Physical Security</b>
<b>7 – Business Continuity</b>	<b>8 – ICT Infrastructure Tools</b>	<b>9 – ICT Implementation Plans</b>



# Risk Assessment & Compliance Audit

- A priority action for the Jamaican Government and major Business will be to assess the current levels of risks & security of computing installations, networks, systems and applications. The following topics should be actively considered and monitored within each audit:

- 1) Management Organization;
- 2) Personnel Security – Vetting & Access Controls
- 3) Software & Applications Security
- 4) Device and Hardware Security
- 5) Network Communications – Access, encryption, fail-over
- 6) Business Continuity and Disaster Recovery (BCP/DR)
- 7) Personal & Business Data Protection
- 8) Cybersecurity Standards and Frameworks
- 9) Physical Building & Facilities Security

*.....Following the initial audit and upgrades for each designated critical computing facility there should be annual audits to check upon the compliance to recommended government cybersecurity standards*





# Data Classification Scheme

- It is highly recommended that data & documents are classified with protective marking (PM) levels similar to the following UK scheme:
  - TOP SECRET
  - SECRET
  - CONFIDENTIAL
  - RESTRICTED
  - PROTECT
  - NOT PROTECTIVELY MARKED
- Access to data & documents whether physical or electronic will then be determined according to rigorously enforced security policies according to the user's vetting level and protective markings



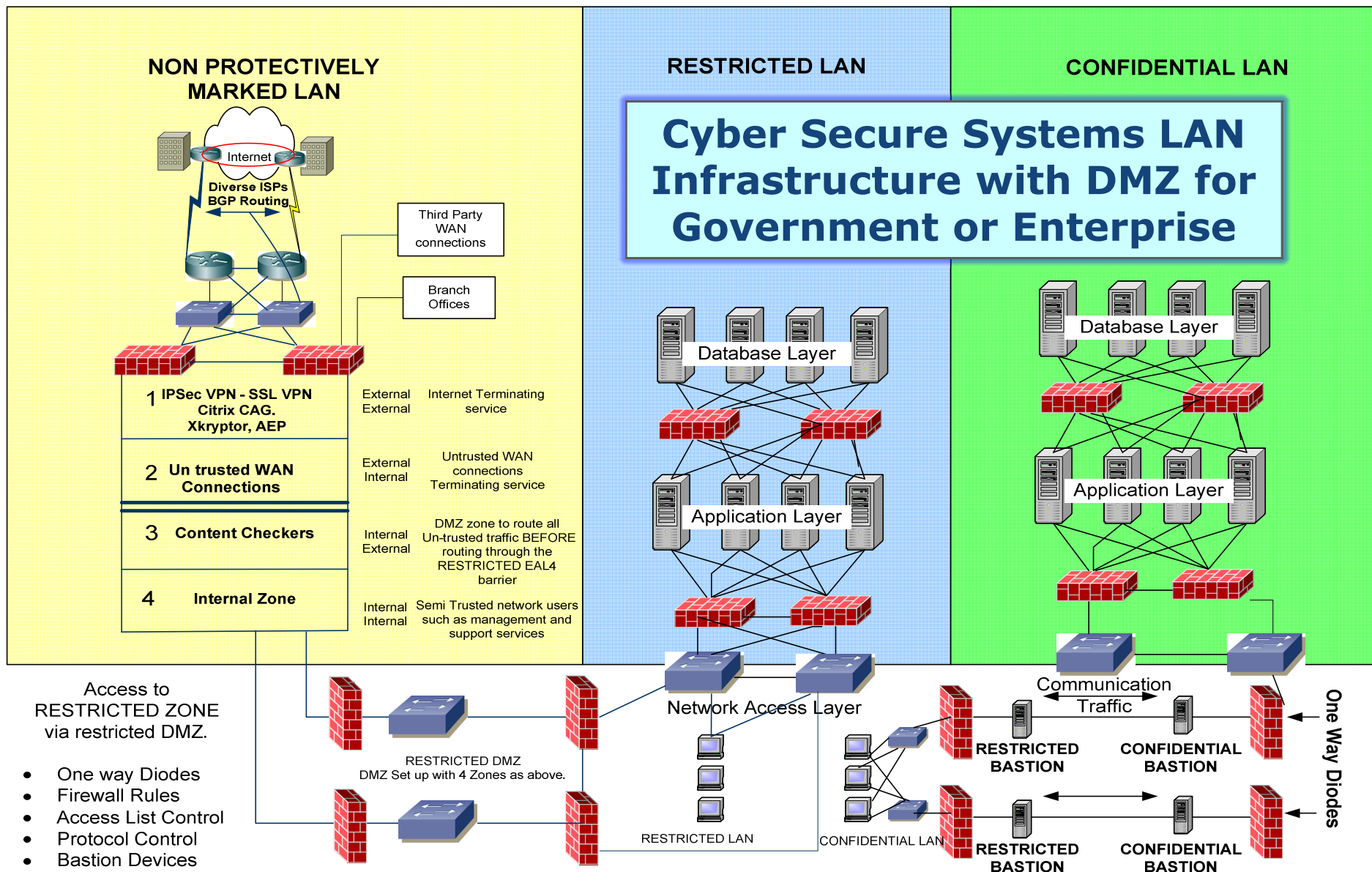
# \* Workshop Session 6 \*

## ITU Global Cybersecurity Agenda: ...*Technological Risks & Solutions*

1 – Technologies & Standards	2 – Sources of Cyber Threats	3 – Risk Assessment Model
4 – Risk Assessment & Audit	5 – Cybersecurity Technologies	6 – Physical Security
7 – Business Continuity	8 – ICT Infrastructure Tools	9 – ICT Implementation Plans



SECURITY OBJECTIVE	CYBERSECURITY TECHNOLOGY		SOLUTION ROLE
Access Control			
Boundary Protection	Firewalls	Aim to prevent unauthorised access to or from a private network.	
	Content Management	Monitor web, messaging and other traffic for inappropriate content such as spam, banned file types and sensitive or classified information.	
Authentication	Biometrics	Biometric systems rely on human body parts such as fingerprints, iris and voice to identify authorised users	
	Smart tokens	Devices such as smart cards with integrated circuit chips (ICC) to store and process authentication details	
Authorisation	User Rights and Privileges	Systems that rely on organisational rules and/or roles to manage access	
System Integrity			
	Antivirus and anti-spyware	A collection of applications that fight malicious software (malware) such as viruses, worms, Trojan Horses etc	
	Integrity Checkers	Applications such as Tripwire that monitor and/or report on changes to critical information assets	
Cryptography			
	Digital Certificates	Rely on Public Key Infrastructure (PKI) to deliver services such as confidentiality, authentication, integrity and non-repudiation	
	Virtual Private Networks	Enable segregation of a physical network in several ‘virtual’ networks	
Audit and Monitoring			
	Intrusion Detection Systems (IDS)	Detect inappropriate, incorrect or abnormal activity on a network	
	Intrusion Prevention Systems (IPS)	Use IDS data to build intelligence to detect and prevent cyber attacks	
	Security Events Correlation Tools	Monitor, record, categorise and alert about abnormal events on network	
	Computer Forensics tools	Identify, preserve and disseminate computer-based evidence	
Configuration Management and Assurance			
	Policy Enforcement Applications	Systems that allow centralised monitoring and enforcement of an organisation’s security policies	
	Network Management	Solutions for the control and monitoring of network issues such as security, capacity and performance	
	Continuity of Operations tools	Backup systems that helps maintain operations after a failure or disaster	
	Scanners	Tools for identifying, analysing and reporting on security vulnerabilities	
	Patch Management	Tools for acquiring, testing and deploying updates or bug fixes	



# \* Workshop Session 6 \*

## ITU Global Cybersecurity Agenda: ...*Technological Risks & Solutions*

1 – Technologies & Standards	2 – Sources of Cyber Threats	3 – Risk Assessment Model
4 – Risk Assessment & Audit	5 – Cybersecurity Technologies	6 – Physical Security
7 – Business Continuity	8 – ICT Infrastructure Tools	9 – ICT Implementation Plans



# Integration with Physical Security

- Cybersecurity for Government & Critical Service Sectors should be tightly integrated with physical security solutions including:
  - 1) Advanced CCTV Camera Surveillance of the Secure Government & Critical Facilities
  - 2) Exterior ANPR (Automatic Number Plate Recognition) Systems for Car Parking & Entrances
  - 3) Integration of the Cyber CERT/CSIRT with physical CCTV & Alarm Control Centres
  - 4) Personnel RFID and/or biometrics office & campus access controls
  - 5) Professionally trained security personnel & guards – 24/7 – for top security facilities
  - 6) Implemented facility security policy for staff, visitors and contractors
  - 7) Intelligent perimeter security controls for campuses and critical service facilities such as airports, power stations, refineries, military bases, hospitals and government institutions
  - 8) On-Line Audit trails and Electronic Log-Files for secure Physical Facilities
  - 9) Focus upon in-depth physical security for computer server rooms, data storage & archives

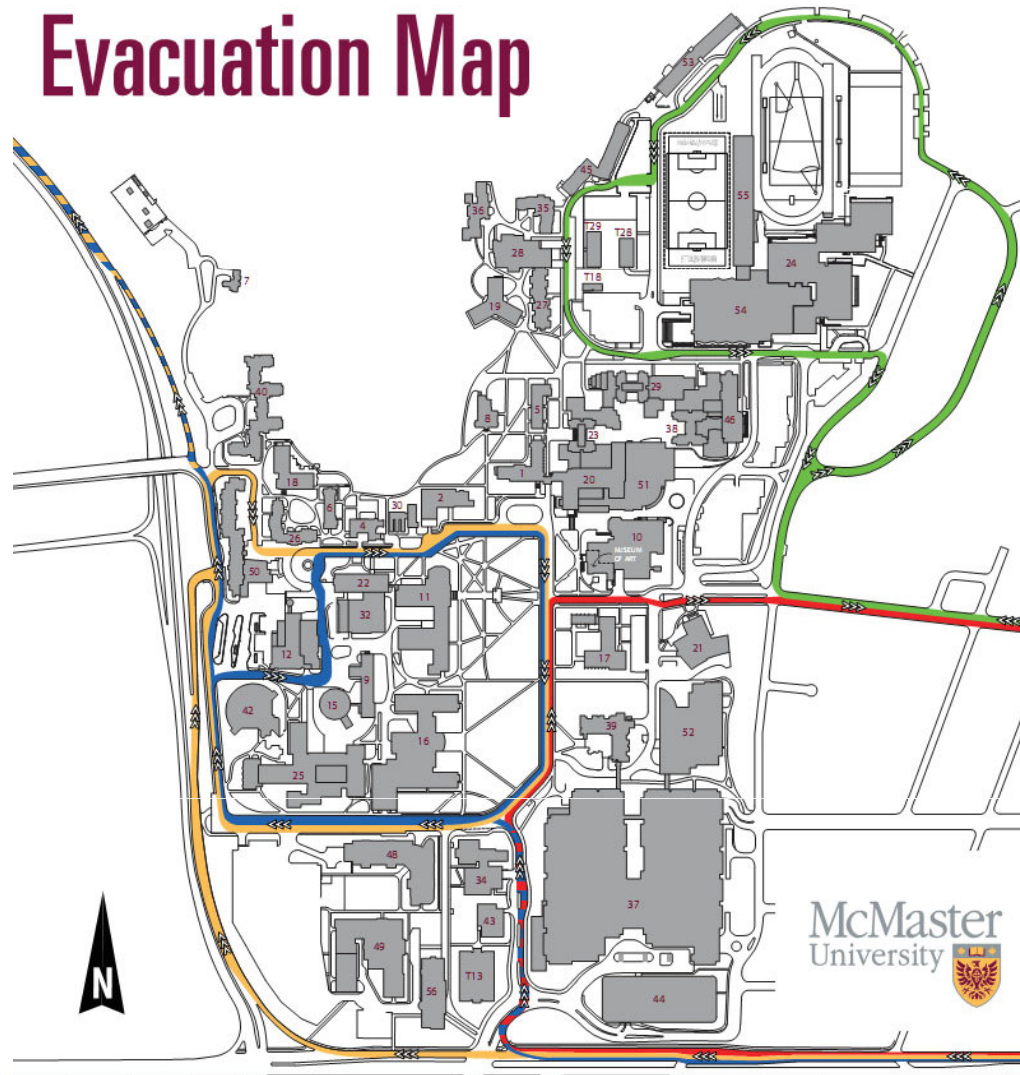
*.....All critical information infrastructures on multi-building campus sites such as airports, universities, hospitals and government agencies require "integrated cyber-physical security"*





# University Campus - Security

## Evacuation Map



### Integrated Campus Security

Access to secure computing facilities and services will need to be managed and integrated within the physical network access & surveillance system



University of Technology,  
Jamaica

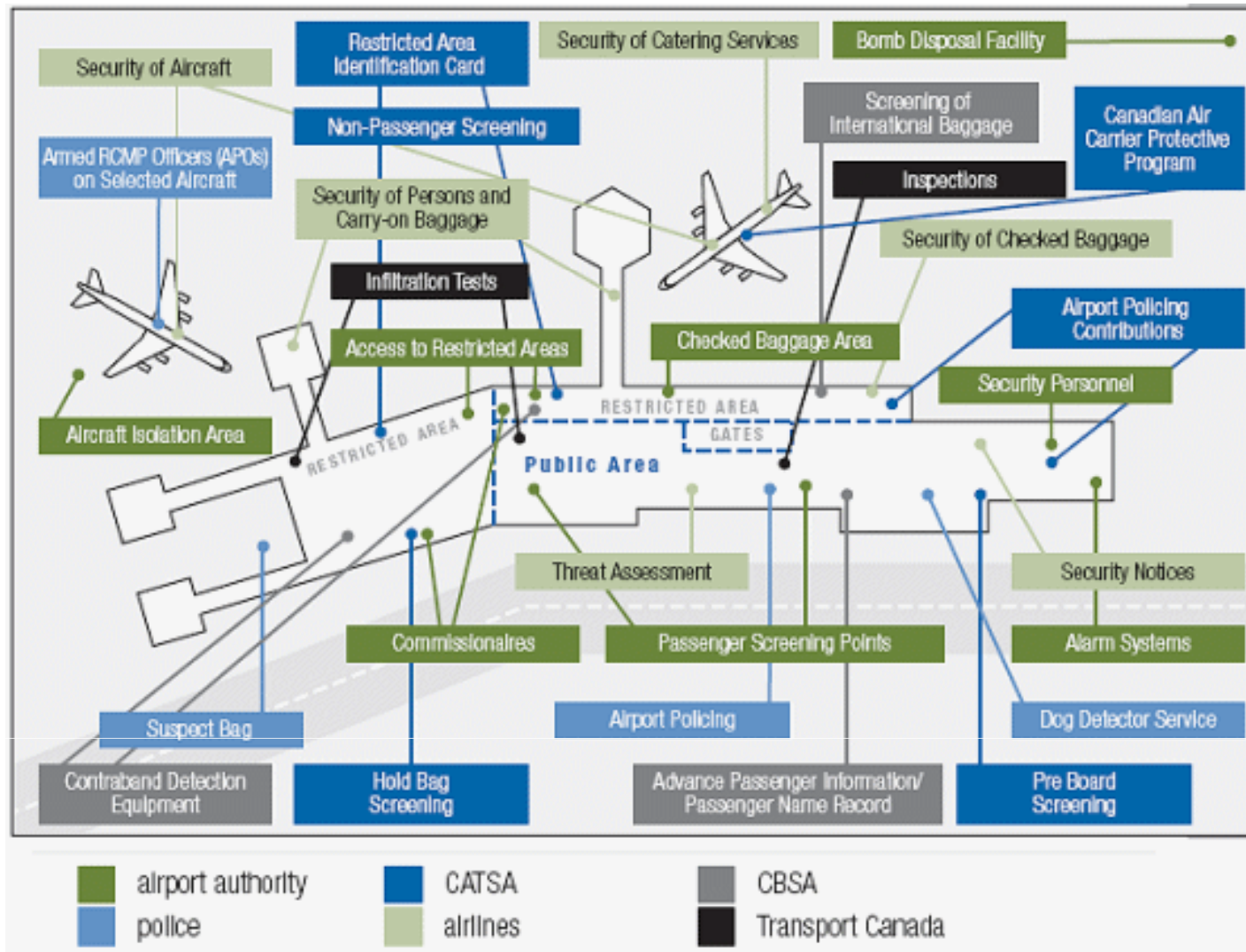
ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



International  
Telecommunication  
Union

Committed to connecting the world

# Airport : Physical Security



## Integrated Airport Security

Airports also require integration of physical and cyber security as well as fully monitored access to the restricted areas & on-line operational computing facilities



# \* Workshop Session 6 \*

## ITU Global Cybersecurity Agenda: ...*Technological Risks & Solutions*

1 – Technologies & Standards	2 – Sources of Cyber Threats	3 – Risk Assessment Model
4 – Risk Assessment & Audit	5 – Cybersecurity Technologies	6 – Physical Security
7 – Business Continuity	8 – ICT Infrastructure Tools	9 – ICT Implementation Plans



# Business Continuity Planning and Disaster Recovery (BCP/DR)

- A key aspect of cybersecurity planning is to ensure that in the event of any form of cyber attack, or even natural event such as earthquake, hurricane, major power failure or terrorist attack that the information and system can be quickly made operational again. So for ALL critical systems it is recommended that:
  - Databases & Servers are continuously mirrored & duplicated in the computer centre
  - Government & Major Enterprise systems should also be fully backed up through a secure remote facility several kms from the city or host institution. This remote system should be networked through duplicate alternative links (maybe fibre and radio)
  - Staff should receive regular “disaster” training exercises so that everyone is ready to take action as soon as a real emergency, whether cyber or natural event, takes place
  - Technological Solutions such as “Virtualisation” and “Cloud Computing” may also be used to increase the resilience and flexibility of the operational systems, but such 21stC solutions will also require additional cybersecurity safeguards and security policies



# \* Workshop Session 6 \*

## ITU Global Cybersecurity Agenda: ...*Technological Risks & Solutions*

1 – Technologies & Standards	2 – Sources of Cyber Threats	3 – Risk Assessment Model
4 – Risk Assessment & Audit	5 – Cybersecurity Technologies	6 – Physical Security
7 – Business Continuity	8 – ICT Infrastructure Tools	9 – ICT Implementation Plans





# ICT Infrastructure Tools & Resources

- The field of cybersecurity tools & standards has only seriously developed since the birth of the Commercial Internet 15 years ago during the mid-90s.
- Some ICT resources that may be of interest to workshop participants include :
  - ITU Technical Cybersecurity Standards – X805 Series, X.1205 Series & others
  - ISO/IEC – 27000 Series including the ISO27001 and ISO27002 recommendations
  - Information Security Forum (ISF) – “Standard of Good Practice for Information Security”
  - Jericho Forum – Focusing on Business Security within the “21stC Open Network & Cloud”
  - NIST – US National Institute of Standards & Technology – “800 Series” focuses on cybersecurity
  - ASIS – US Organisation that focuses on all aspects of physical & cyber enterprise security
  - ITU “Botnet” Mitigation Toolkit – Jan 2008 – Important toolkit to minimise DDOS attacks
  - Other standards organisations concerned with cybersecurity include: IETF, ETSI, IEEE, & 3GPP
- We’ll be exploring technical standards, architectures and solutions in-depth during the following 2-Day ITU Technology Workshop on 16<sup>th</sup>/17<sup>th</sup> Sept



# Info Security Forum Matrix – (1)

Topic	SM	CB	CI	NW	SD
User authentication			CI4.5 User authentication		
User authorisation			CI4.2 User authorisation		
Virus protection	SM5.1 Virus protection				
Web-enabled applications		CB6.4 Web-enabled applications			SD4.6 Web-enabled development
Wireless access				NW2.4 Wireless access	
Workstation configuration		CB3.3 Workstation configuration	CI2.4 Workstation configuration		

SM = Security Management  
 CB = Critical Business Applications  
 CI = Computer Installations  
 NW = Networks  
 SD = Systems Development



# Info Security Forum Matrix – (2)

Topic	SM	CB	CI	NW	SD
Access control		CB3.1 Access control	CI4.1 Access control arrangements CI4.3 Access privileges		
Acquisition					SD4.4 Acquisition
Application controls		CB2.2 Application controls			SD4.2 Application controls
Asset management	SM4.3 Asset management		CI1.3 Asset management		
Availability requirements		CB1.3 Availability requirements			SD3.4 Availability requirements
Back-up		CB4.4 Back-up	CI3.2 Back-up	NW3.5 Back-up	
Business continuity	SM4.5 Business continuity	CB2.5 Business continuity	CI6.1 Contingency plan CI6.2 Contingency arrangements CI6.3 Validation and maintenance	NW3.6 Service continuity	
Change management		CB2.3 Change management	CI3.3 Change management	NW3.2 Change management	
Confidentiality requirements		CB1.1 Confidentiality requirements			SD3.2 Confidentiality requirements
Configuring network devices				NW2.1 Configuring network devices	
Cryptography	SM6.1 Use of cryptography	CB6.2 Cryptographic key management			
Development methodologies and environment					SD1.2 Development methodology SD1.4 Development environments
E-mail	SM6.3 E-mail				
Electronic commerce	SM6.6 Electronic commerce				



# Info Security Forum Matrix – (3)

Topic	SM	CB	CI	NW	SD
Emergency fixes			CI3.5 Emergency fixes		
Event logging			CI2.2 Event logging		
External access/ connections		CB4.3 External connections		NW2.3 External access	
Firewalls				NW2.2 Firewalls	
Forensic investigations	SM5.5 Forensic investigations				
General security controls					SD4.3 General security controls
Handling information		CB2.6 Sensitive information	CI3.1 Handling computer media		
Hazard protection			CI2.6 Hazard protection		
Host system configuration			CI2.3 Host system configuration		
Incident management	SM5.4 Emergency response	CB2.4 Incident management	CI3.4 Incident management	NW3.3 Incident management	
Information privacy	SM4.2 Information privacy				
Information security function	SM2.2 Information security function				
Installation and network design			CI2.1 Installation design	NW1.2 Network design	
Instant Messaging	SM 6.8 Instant Messaging				
Installation process					SD6.2 Installation process
Integrity requirements		CB1.2 Integrity requirements			SD3.3 Integrity requirements
Intrusion detection	SM5.3 Intrusion detection				



# Info Security Forum Matrix – (4)

Topic	SM	CB	CI	NW	SD
Local security co-ordination	SM2.3 Local security co-ordination	CB5.1 Local security co-ordination	CI5.1 Local security co-ordination	NW4.1 Local security co-ordination	SD2.1 Local security co-ordination
Management commitment	SM1.1 Management commitment SM2.1 High-level control				
Malicious mobile code protection	SM5.2 Malicious mobile code protection				
Network documentation				NW1.4 Network documentation NW5.1 Voice network documentation	
Outsourcing	SM6.7 Outsourcing				
Patch Management	SM 5.6 Patch management		CI3.6 Patch management		
Physical protection	SM4.4 Physical protection		CI2.8 Physical access	NW3.4 Physical security	
Post-implementation review					SD6.3 Post-implementation review
Power supplies			CI2.7 Power supplies		
Public key infrastructure	SM6.2 Public key infrastructure	CB6.3 Public key infrastructure			
Quality assurance					SD1.3 Quality assurance
Remote maintenance				NW3.7 Remote maintenance	
Remote working	SM6.4 Remote working				
Resilience		CB4.2 Resilience	CI2.5 Resilience	NW1.3 Network resilience NW5.2 Resilience of voice networks	
Risk analysis/assessment	SM3.3 Information risk analysis	CB5.3 Information risk analysis	CI5.4 Information risk analysis	NW4.4 Information risk analysis	SD3.5 Information risk assessment
Roles and responsibilities	SM3.2 Ownership	CB2.1 Roles and responsibilities	CI1.1 Roles and responsibilities	NW1.1 Roles and responsibilities	SD1.1 Roles and responsibilities



# Info Security Forum Matrix – (5)

Topic	SM	CB	CI	NW	SD
Security architecture	SM4.1 Security architecture				
Security audit/review	SM7.1 Security audit/review	CB5.4 Security audit/review	CI5.5 Security audit/review	NW4.5 Security audit/review	SD2.3 Security audit/review
Security awareness	SM2.4 Security awareness	CB3.4 Security awareness	CI5.2 Security awareness	NW4.2 Security awareness	SD2.2 Security awareness
Security classification	SM3.1 Security classification	CB5.2 Security classification	CI5.3 Security classification	NW4.3 Security classification	
Security education	SM2.5 Security education				
Security monitoring	SM7.2 Security monitoring				
Security policy	SM1.2 Security policy				
Service providers		CB4.1 Service agreements	CI1.2 Service agreements	NW1.5 Service providers	
Sign-on process		CB3.2 Application sign-on process	CI4.4 Sign-on process		
Special controls				NW5.3 Special voice network controls	
Specifications of requirements					SD3.1 Specification of requirements
Staff agreements	SM1.3 Staff agreements				
System design/build					SD4.1 System design SD4.5 System build
System network monitoring			CI1.4 System monitoring	NW3.1 Network monitoring	
System promotion criteria					SD6.1 System promotion criteria
Testing					SD5.1 Testing process SD5.2 Acceptance testing
Third party access	SM6.5 Third party access	CB6.1 Third party agreements			



# ITU Botnet Mitigation Toolkit





# ITU Technical Security Standards

- The ITU Technical Families of Security Standards are extremely comprehensive and span most aspects of government and enterprise cybersecurity systems and architectures.
- The standards are also being continuously developed and upgraded by professional specialists from the ICT Industry, Government & Academia
  - *X.805* – Security Architecture for End-to-End Communications
  - *X.1205* – Overview of Cybersecurity and General Guidelines
  - *X.1250* – Security Standards for Identity Management
  - *X.509* – Public Key Infrastructure & Certificate Frameworks
  - *H.323* – Multimedia Systems Security
  - *J.170* – Security Specifications for TV & Multimedia Cable Networks
- The ITU security standards can be freely downloaded by the ITU website



# **\* Workshop Session 6 \***

## **ITU Global Cybersecurity Agenda: ...*Technological Risks & Solutions***

<b>1 – Technologies &amp; Standards</b>	<b>2 – Sources of Cyber Threats</b>	<b>3 – Risk Assessment Model</b>
<b>4 – Risk Assessment &amp; Audit</b>	<b>5 – Cybersecurity Technologies</b>	<b>6 – Physical Security</b>
<b>7 – Business Continuity</b>	<b>8 – ICT Infrastructure Tools</b>	<b>9 – ICT Implementation Plans</b>



# ICT CyberSecurity Plans : Next Steps

- The following next steps are suggested for Jamaica in order to meet the requirement of the ITU GCA - Technical & Procedural Measures:
  - Establish the National Cybersecurity Agency
  - Discuss and Agree the Multi-Year Investment Budget
  - Recruit Top-Level Cybersecurity Technical Specialist
  - Organise Professional Cybersecurity Training Courses
  - Undertake in-depth technical audit of ALL Government ICT facilities as well as those of critical organisations such as telco & mobile operators, airports, power stations & hospitals
  - Based upon “Best Practice” develop practical plans to upgrade existing ICT facilities to meet and to comply with international cybersecurity standards including ITU & ISO/IEC
  - Implement the ICT upgrades across the government & critical sector facilities
  - Introduce annual compliance audits for all critical ICT facilities
  - Continue professional cybersecurity training through Degree Level & Master Level University Courses, as well as regular “refresher” courses for operational security staff

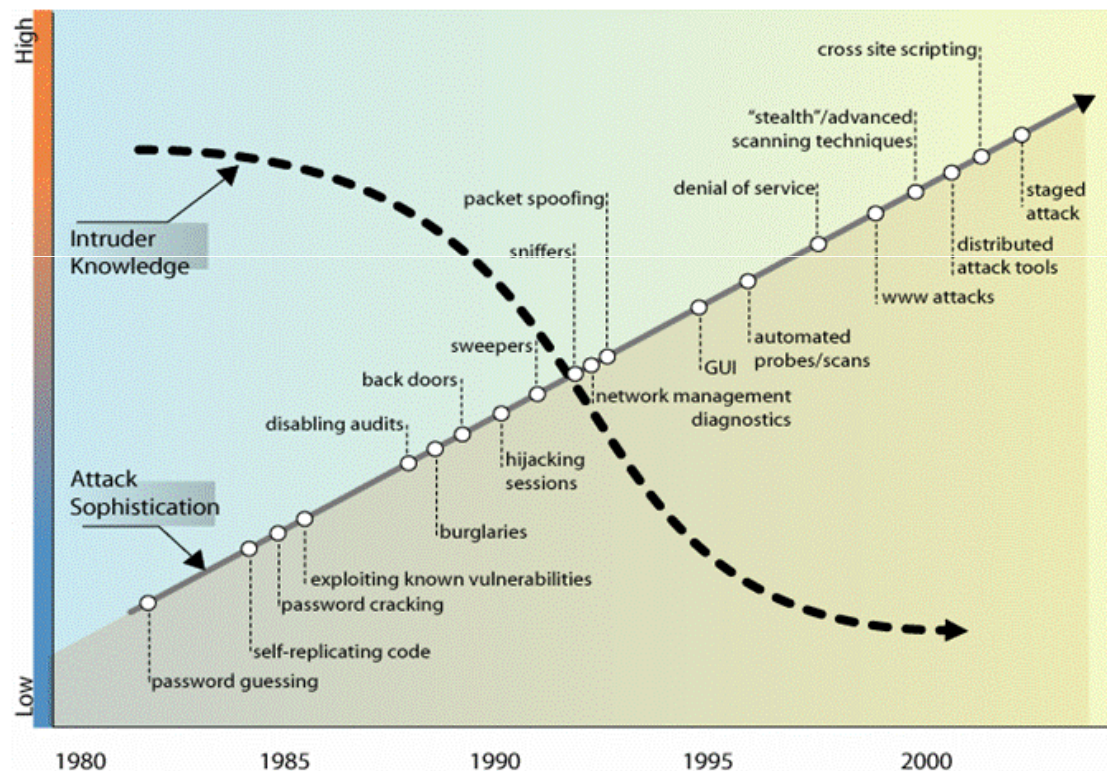


# GCA: Technical & Procedural Measures

GCA PILLAR: TECHNICAL AND PROCEDURAL MEASURES		
Corresponding GCA Goal	Goal 1	Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for hardware and software applications and systems.
	Goal 2	Development of global strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organisational structures to ensure the recognition of digital credentials across geographical boundaries
Deliverables		<p>The Recommendations under this pillar include:</p> <ul style="list-style-type: none"> <li>• Linking technical solutions to accepted security criteria and accreditation schemes</li> <li>• Generic technical and networking solutions required to create a digital identity system and necessary organisational structures</li> </ul>



# Attack Sophistication v. Intruder Knowledge



Source: [www.cert.org](http://www.cert.org)



6



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



International  
Telecommunication  
Union

Committed to connecting the world



# \* ITU Cybersecurity Strategy \*

## *"3-Day Workshop Overview"*

<b>S1- Mon: 9:30-11:00</b>  <b>"The Cybersecurity Challenge!..."</b>	<b>S2-Mon: 11:30-13:00</b>  <b>"The Need for Action!"</b>	<b>S3 - Mon:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Cybersecurity Action Plans"</b>	<b>S4 - Mon:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Cybersecurity Action Plans"</b>
<b>S5- Tues: 9:30-11:00</b>  <b>ITU Cyber Agenda: 1</b> <b>"Cybercrime and Legislation"</b>	<b>S6-Tues: 11:30-13:00</b>  <b>ITU Cyber Agenda: 2</b> <b>"Technological Risks and Solutions"</b>	<b>S7 -Tues:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Legislation and Regulations"</b>	<b>S8 -Tues:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Legislation and Regulations"</b>
<b>S9- Wed: 9:30-11:00</b>  <b>ITU Cyber Agenda: 3</b> <b>"Operational Risks and Organisational Structures"</b>	<b>S10-Wed:11:30-13:00</b>  <b>ITU Cyber Agenda: 4&amp;5</b> <b>"Capacity Building and Collaboration"</b>	<b>S11-Wed:14:00-15:30</b> <b>Group Session:</b>  <b>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</b>	<b>S12-Wed:16:00-17:30</b> <b>Group Session:</b>  <b>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</b>





# \* Group Workshop Session 7 \*

## Developing National Legislation & Regulations

- Team Worksheet – Cyber Legislation, Policies and Regulations
  - *Task 1* – Select your Critical Sector: Govt, Banks, Telco, Transport, Energy
  - *Task 2* – List Potential CyberCrimes and CyberThreats such as ID Theft
  - *Task 3* – Structure the Cybercrimes as eTheft, eTerrorism, eSpying.....
  - *Task 4* – Review the “Best Practice” Laws and ITU Cybercrime Kit
  - *Task 5* – Discuss the ways in which traditional laws need upgrading
  - *Task 6* – Brainstorm new Policies and Regulations to combat Cybercrime
  - *Task 7* – Decide specific Actions against the Cybercrime List from Task 1
  - *Task 8* – Prepare a short presentation & slides with your Recommendations!

*.....Stay practical and focus on ideas and examples of “Best Practice” Legislation & Regulations presented during the morning presentation. Also browse through the excellent ITU Cybercrime Toolkit for more ideas & actions!*



# \* Group Workshop Session 7\*

## Developing National Legislation, and Regulations

### Suggested Time Allocations for Task Actions: 90mins

<b>1 – Task Assignment: Choose your Critical Service Sector:</b>  <i>Government, Banking/Finance Telecomms, Transport, Energy</i>	<b>Task 2 – Identify and List the Cybercrimes that could impact your chosen critical sector</b>	<b>Task 3 – Structure the Potential Cybercrimes as:</b>  eTheft, eTerrorism, Forgery/Fraud Computer Misuse, Copyright etc
<b>Task 4– Review “Best Practice” &amp; download ITU Cybercrime Toolkit &amp; Legal Templates</b>	<b>Task 5 – Consider the ways that current laws need to be upgraded to fight cybercrime</b>	<b>Task 6 – Brainstorm new laws and regulations to combat cybercrime in your sector</b>
<b>Task 7 – Decide specific actions against cybercrime from your sector lists in (2) &amp; (3)</b>	<b>Task 8 – Prepare Short 10 Min Presentation of Suggestions</b>	<b>Task 8 – Prepare Short 10min Presentation of Suggestions</b>

**Note: Each Task Time Segment = 10Mins**

# Key to Cybersecurity Workshop Session

## Colour-Code Classifications: Interactive Tasks

Colour Code Workshop	RED	ORANGE	YELLOW	BLUE	GREEN
<b>Monday</b> <b>-Action Plans -</b>	(1) Legal	(2) Technical	(3) Organisation	(4) Capacity	(5) International
<b>Tuesday</b> <b>- Laws -</b>	<b>Information Disclosure</b>	<b>Computer Misuse</b>	<b>Forgery &amp; ID Fraud</b>	<b>Information Interception</b>	<b>Copyright &amp; Patents Law</b>
<b>Wednesday</b> <b>- Road Map -</b>	Q1-2011	Q2-2011	Q3-2011	Q4-2011	FY2012
<b>Thursday</b> <b>- ICT Security-</b>	Unauthorised Info Access	DDoS-Denial of Services	MALWARE	Disclosure & Misuse	Info Access & Exploitation
<b>Friday</b> <b>- Sector Security -</b>	Cyber Criminal Threat	Cyber Terrorist Threat	Malicious Hacking & Exploitation	Internal Operational Threat	Natural Disaster or Other Event



# \* ITU Cybersecurity Strategy \*

## *"3-Day Workshop Overview"*

<b>S1- Mon: 9:30-11:00</b>  <b>"The Cybersecurity Challenge!..."</b>	<b>S2-Mon: 11:30-13:00</b>  <b>"The Need for Action!"</b>	<b>S3 - Mon:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Cybersecurity Action Plans"</b>	<b>S4 - Mon:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Cybersecurity Action Plans"</b>
<b>S5- Tues: 9:30-11:00</b>  <b>ITU Cyber Agenda: 1</b> <b>"Cybercrime and Legislation"</b>	<b>S6-Tues: 11:30-13:00</b>  <b>ITU Cyber Agenda: 2</b> <b>"Technological Risks and Solutions"</b>	<b>S7 -Tues:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Legislation and Regulations"</b>	<b>S8 -Tues:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Legislation and Regulations"</b>
<b>S9- Wed: 9:30-11:00</b>  <b>ITU Cyber Agenda: 3</b> <b>"Operational Risks and Organisational Structures"</b>	<b>S10-Wed:11:30-13:00</b>  <b>ITU Cyber Agenda: 4&amp;5</b> <b>"Capacity Building and Collaboration"</b>	<b>S11-Wed:14:00-15:30</b> <b>Group Session:</b>  <b>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</b>	<b>S12-Wed:16:00-17:30</b> <b>Group Session:</b>  <b>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</b>



\* **Group Workshop Session 8\***  
**Team Discussion: National Laws & Regulations**  
**Schedule: Task Presentations = 90mins**

Group 1 = Government	Group 1 = Government	Group 2 = Banking/Finance
Group 2 = Banking/Finance	Group 3 = Telecomms/Mobile	Group 3 = Telecomms/Mobile
Group 4 = Transport or Energy	Group 4 = Transport or Energy	Group Discussion & Summary

**Note: Each Task Time Segment = 10Mins**

# \* ITU Cybersecurity Strategy \*

## *"3-Day Workshop Overview"*

<b>S1- Mon: 9:30-11:00</b>  <b>"The Cybersecurity Challenge!..."</b>	<b>S2-Mon: 11:30-13:00</b>  <b>"The Need for Action!"</b>	<b>S3 - Mon:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Cybersecurity Action Plans"</b>	<b>S4 - Mon:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Cybersecurity Action Plans"</b>
<b>S5- Tues: 9:30-11:00</b>  <b>ITU Cyber Agenda: 1</b> <b>"Cybercrime and Legislation"</b>	<b>S6-Tues: 11:30-13:00</b>  <b>ITU Cyber Agenda: 2</b> <b>"Technological Risks and Solutions"</b>	<b>S7 -Tues:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Legislation and Regulations"</b>	<b>S8 -Tues:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Legislation and Regulations"</b>
<b>S9- Wed: 9:30-11:00</b>  <b>ITU Cyber Agenda: 3</b> <b>"Operational Risks and Organisational Structures"</b>	<b>S10-Wed:11:30-13:00</b>  <b>ITU Cyber Agenda: 4&amp;5</b> <b>"Capacity Building and Collaboration"</b>	<b>S11-Wed:14:00-15:30</b> <b>Group Session:</b>  <b>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</b>	<b>S12-Wed:16:00-17:30</b> <b>Group Session:</b>  <b>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</b>





# **\* Workshop Session 9 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Operational Risks and Organisational Structures***

<b>1 – Structures and Strategies</b>	<b>2 - Cybersecurity Co-ordination</b>	<b>3 – National Cyber Agency</b>
<b>4 – Cyber Agency Case Studies</b>	<b>5 – Models for Cyber Agencies</b>	<b>6 – National Roll-Out Plans</b>
<b>7 – Emergency Response - CERT</b>	<b>8 – National Cybercrime Unit</b>	<b>9 – Benefits for Jamaica</b>



# **\* Workshop Session 9 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Operational Risks and Organisational Structures***

<b>1 – Structures and Strategies</b>	<b>2 - Cybersecurity Co-ordination</b>	<b>3 – National Cyber Agency</b>
<b>4 – Cyber Agency Case Studies</b>	<b>5 – Models for Cyber Agencies</b>	<b>6 – National Roll-Out Plans</b>
<b>7 – Emergency Response - CERT</b>	<b>8 – National Cybercrime Unit</b>	<b>9 – Benefits for Jamaica</b>



# Structures and Strategies

- *National Cybersecurity Strategy:* The Jamaican Government first needs to define and communicate its cybersecurity strategy. This strategy will most likely to be associated with existing plans for e-Government
- *National Cybersecurity Agency (NCA):* An effective government agency closely linked to the Cabinet and Ministry of Security is required to co-ordinate resources, and to roll-out the national cybersecurity roadmap
- *Enterprise Organisations:* Businesses will also need to consider the implementation and management of enterprise-wide cybersecurity through the appointment of a Chief Security Officer (CSO) working alongside the Chief Information Officer (CIO)
- *Specialised Cybersecurity Organisations:* There is also a requirement for dedicated organisations such as a national CERT (Computer Emergency Response Team), and National Cybercrime Unit (NCU)

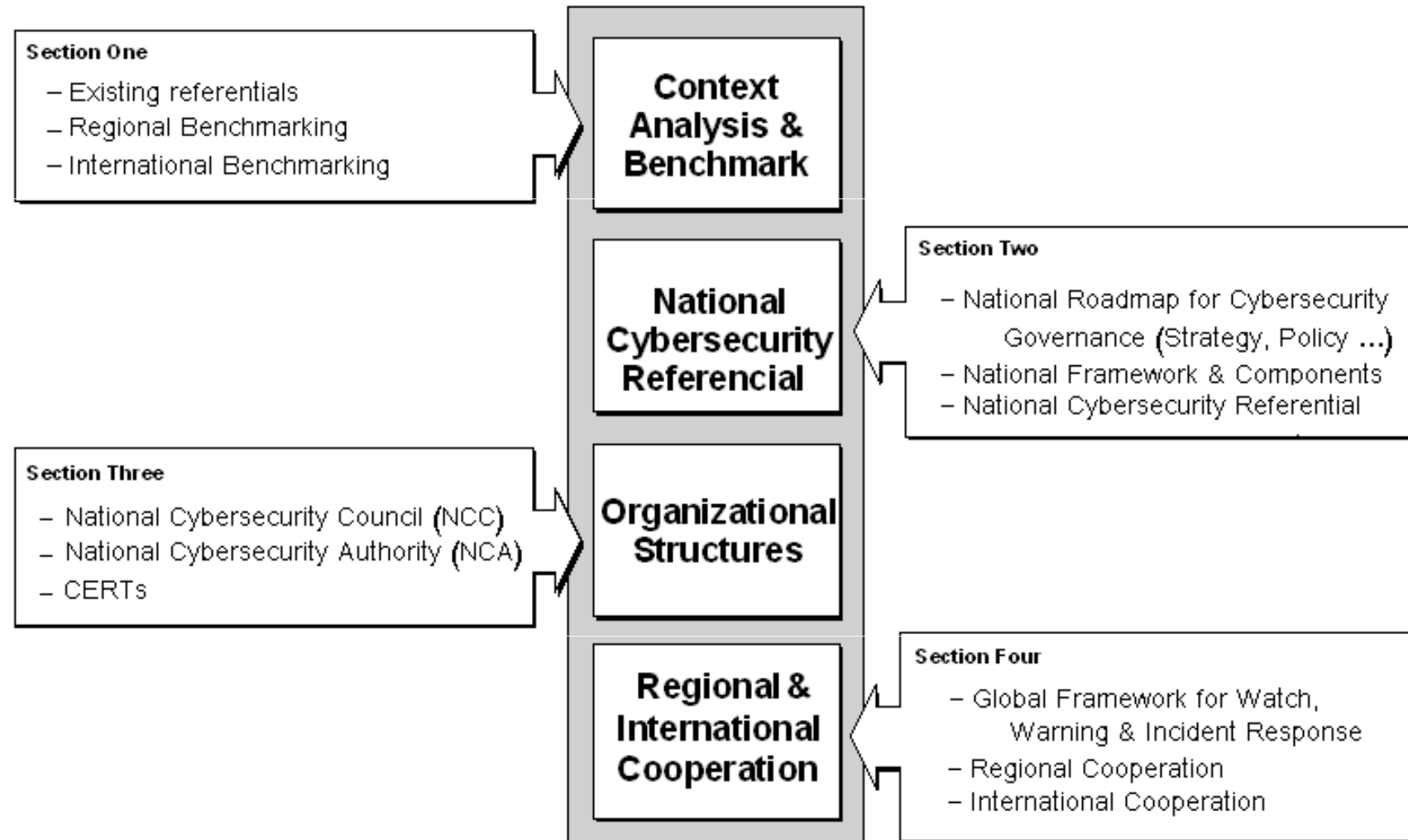


# ITU - GCA: Organisational Structure Goals

GCA PILLAR: ORGANISATIONAL STRUCTURES		
Corresponding GCA Goal	Goal 1	Elaboration of global strategies for the creation of appropriate national and regional <b>organisational structures</b> and policies on <b>cybercrime</b>
	Goal 2	Development of strategies for the creation of a global framework for <b>watch, warning and incident response</b> to ensure cross-border coordination between new and existing initiatives
	Goal 3	Development of a global strategy to facilitate <b>human and institutional capacity building</b> to enhance knowledge and know-how across sectors and in all the above-mentioned areas
Deliverables		<p>The Recommendations under this pillar include:</p> <p>(1) Creation of appropriate national organisational structures and policies on cybercrime starting with the National Cybersecurity Agency</p> <p>(2) The development of a national framework for watch, warning and incident response</p> <p>(3) The development of institutional capacity in Jamaica to train a cadre of cybersecurity professionals in Managerial, Technical and Information Assurance areas</p> <p>(4) Strategy for participation in international cybersecurity activities</p>



# An Approach to Organisational Structures for National Cybersecurity



# \* Workshop Session 9 \*

## ITU Global Cybersecurity Agenda:

### *...Operational Risks and Organisational Structures*

1 – Structures and Strategies	2 - Cybersecurity Co-ordination	3 – National Cyber Agency
4 – Cyber Agency Case Studies	5 – Models for Cyber Agencies	6 – National Roll-Out Plans
7 – Emergency Response - CERT	8 – National Cybercrime Unit	9 – Benefits for Jamaica





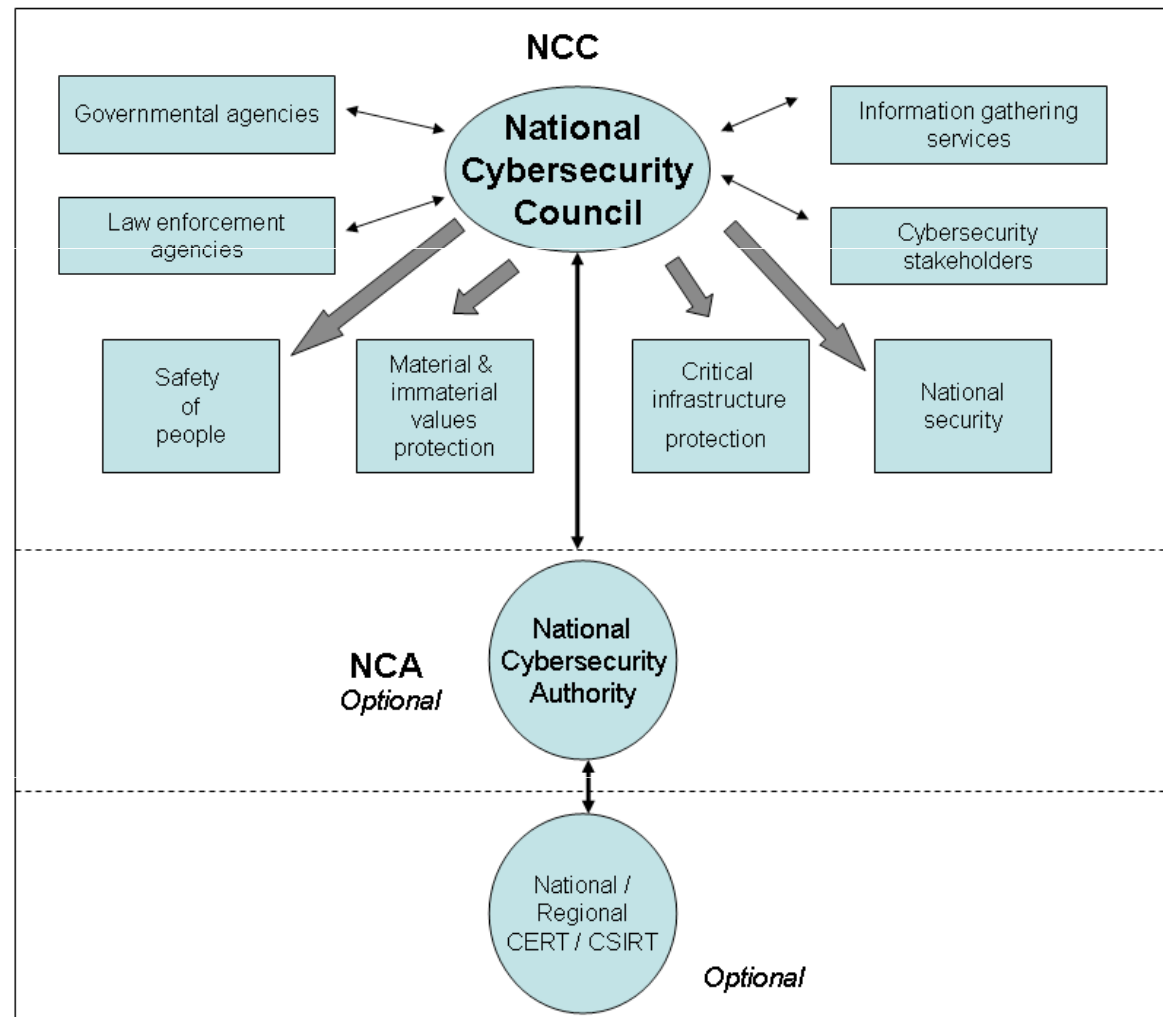
# Cybersecurity Co-ordination

- The proposed National Security Agency (or Council) is responsible for the co-ordination of all actions & programmes:
  - 1) Liaison with all the Jamaican Government Ministries & Agencies
  - 2) Co-ordination with Regional & Local Government Organisations
  - 3) Leadership for the Cybersecurity Training and Awareness Programmes
  - 4) Partnerships with Private Business to promote secure eBusiness / eTrade
  - 5) Development and Implementation of Cybercrime Legislation & Regulations
  - 6) Working with the police & military regarding cybercrime / cyberterrorism
  - 7) International Collaboration and Partnerships such as the ITU and Interpol
  - 8) Establish of National CERT/CSIRT for 24/7 Jamaican Cyberspace Monitoring
  - 9) Work with Critical Service Sectors such as Banking/Finance, Telecomms, Energy, Education, Healthcare and Travel/Tourism to upgrade cybersecurity

.....We'll consider each of these requirements during the course of this session!



# Framework for Organisational Structures



# \* Workshop Session 9 \*

## ITU Global Cybersecurity Agenda:

### *...Operational Risks and Organisational Structures*

1 – Structures and Strategies	2 - Cybersecurity Co-ordination	3 – National Cyber Agency
4 – Cyber Agency Case Studies	5 – Models for Cyber Agencies	6 – National Roll-Out Plans
7 – Emergency Response - CERT	8 – National Cybercrime Unit	9 – Benefits for Jamaica



# National Cyber Agency (NCA)

- We'll briefly consider and summarise the organisation & strategies of the National Cybersecurity Agencies for :
  - *UK Government* - Cybersecurity Strategy for the UK – Safety, Security & Resilience in Cyberspace (UK Office of Cybersecurity – June 2009)
  - *USA Government* - Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure – May 2009
  - *Australian Government* - Australian Cybersecurity Policy and Co-ordination Committee (CSPC – Nov 2009), within Attorney-General's Government Dept
  - *Malaysian Government* - "Cybersecurity Malaysia" – Mosti : Ministry of Science, Technology & Innovation, and includes the MyCERT & Training Centre
- ... *There are other national agency case studies that we could consider but they all have the common feature that they are driven from the highest level of government and include the 24/7 management of cyber incidents and alerts.*



# Business Continuity: Event Impact Analysis

Threat or Trigger	Likelihood (Rate 1-5)	X	Impact (Rate 1-5)	=	Relative Weight
	<i>1 = Very Low</i> <i>2 = Low</i> <i>3 = Medium</i> <i>4 = High</i> <i>5 = Very High</i>		<i>1 = Negligible</i> <i>2 = Some</i> <i>3 = Moderate</i> <i>4 = Significant</i> <i>5 = Severe</i>		
Earthquake		X		=	
Power Failure		X		=	
Fire		X		=	
Hurricane		X		=	
Flood		X		=	
Bombing		X		=	
NBC* Attack at Site		X		=	
NBC* Attack within 50 miles		X		=	
Cyber Attack		X		=	
Kidnapping		X		=	
Sabotage		X		=	
Hazmat Accident		X		=	
Product Recall		X		=	
Public Health		X		=	
Work Stoppage		X		=	

\*Nuclear, Biological, and Chemical



# Chief Security Officer : Profile

## Chief Security Officer (CSO) Guideline

### 12.1 Model Profile of a Chief Security Officer Function

Risks	Potential Processes & Services	Skill Set Required
Human Resources & Intellectual Assets	Global Security Policy & Procedures Administration	<b>Relationship Manager</b> <i>Develops, influences and nurtures trust-based relationships with business unit leaders, government officials and professional organizations. Acts as a consultant to all organizational clients.</i>
Ethics & Reputation	Technology & Infrastructure Protection	<b>Executive Management &amp; Leadership</b> <i>Builds, motivates and leads a professional team attuned to organizational culture, responsive to business needs and committed to integrity and excellence.</i>
Financial Assets	Information Risk Management	
Information Technology (IT) Systems	Business Continuity, Crisis Management & Response	<b>Subject Matter Expert</b> <i>Provides or sees to the provision of technical expertise appropriate to knowledge of risk and the cost-effective delivery of essential security services.</i>
Transportation, Distribution & Supply Chain	Employee Risk Awareness	
Legal, Regulatory & General Counsel	Investigative & Forensic Services	<b>Governance Team Member</b> <i>Provides intellectual leadership and active support to the organization's governance team to ensure risks are made known to senior management and the Board.</i>
Physical & Premises	Safe & Secure Workplace Operations	
Environmental, Health & Safety **	Tailored Business-Process Safeguards	<b>Risk Manager</b> <i>Identifies, analyzes and communicates on business and security-related risks to the organization.</i>
	Insurance & Risk Transfer	
	Risk Assessment, Evaluation & Testing	<b>Strategist</b> <i>Develops global security strategy keyed to likely risks and in collaboration with organization's stakeholders.</i>
	Executive Protection	
	Background & Due Diligence Investigations	<b>Creative Problem Solver</b> <i>Aids competitiveness and adds value by enabling the organization to engage in business processes to mitigate risk. Acts as a positive change agent on behalf of organizational protection.</i>
	Business Conduct & Security Compliance	
	External & Government Relations	
	Business Intelligence & Counter-Intelligence Support	

\*\* Recognizing that EH&S may be structured outside the scope of security functions, there are still significant risk issues to an organization. Since many organizations have combined their EH&S and security functions, we have chosen to present it in this Guideline for consideration.





# **\* Workshop Session 9 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Operational Risks and Organisational Structures***

<b>1 – Structures and Strategies</b>	<b>2 - Cybersecurity Co-ordination</b>	<b>3 – National Cyber Agency</b>
<b>4 – Cyber Agency Case Studies</b>	<b>5 – Models for Cyber Agencies</b>	<b>6 – National Roll-Out Plans</b>
<b>7 – Emergency Response - CERT</b>	<b>8 – National Cybercrime Unit</b>	<b>9 – Benefits for Jamaica</b>



# UK Government : Office of Cybersecurity (OCS)

The UK Government Office of Cybersecurity (OCS) has eight well defined work streams as follows:

- 1) Safe, Secure and Resilient Systems
- 2) Policy, Legal and Regulatory Issues
- 3) Awareness and Culture Change
- 4) Cybersecurity Skills and Education
- 5) Technical Capabilities and R&D
- 6) Exploitation of UK Capabilities
- 7) International Engagement & Partnership
- 8) Governance, Roles and Responsibilities

*...these include the further development of The UK response to Cybercrime through the Association Chief Police Officers (ACPO)*

The Government will...

**"Secure the UK's advantage in cyber space ...**

**...by reducing risk from the UK's use of cyber space...**

- Reduce the threat of cyber operations by reducing an adversary's motivation and capability;
- Reduce the vulnerability of UK interests to cyber operations;
- Reduce the impact of cyber operations on UK interests;

**...and exploiting opportunities in cyber space...**

- Gather intelligence on threat actors;
- Promote support for UK policies; and
- Intervene against adversaries;

**...through improving knowledge, capabilities and decision-making.**

- Improve knowledge and awareness;
- Develop doctrine and policy;
- Develop governance and decision making;
- Enhance technical and human capabilities.



# US Government : Office of CyberSecurity (CS&C)

- Following the June 2009, US Government Policy Review, the Department of Homeland Security (DHS) has responsibility for hosting the "*Office of Cybersecurity and Communications*" (CS&C). Within this large organisation is the "*National Cyber Security Division*" (NCSD):

- *National Cyberspace Response System*

- National Cyber Alert System
- US-CERT Operations
- National Cyber Response Co-ordination Group
- Cyber Cop Portal (for investigation and prosecution of cyber attacks)

- *Federal Network Security*

- Ensuring the maximum security of executive civilian departments and agencies

- *Cyber-Risk Management Programs*

- Cyber Exercises: Cyber Storm
- National Outreach Awareness
- Software Assurance Program

....The US Government DHS also has a National Cyber Security Center (NCSC) which is tasked with the protection of the US Government's Communications Networks



# Australian Government : CSPC

- The **Cyber Security Policy and Coordination (CSPC) Committee** is the Australian Government committee that coordinates the development of cyber security policy for the Australian Government. The CSPC Committee:
  - Provides whole of government strategic leadership on cyber security
  - Determines priorities for the Australian Government
  - Coordinates the response to cyber security events
  - Coordinates Australian Government cyber security policy internationally.



Cyber Security Operations Centre (CSOC)

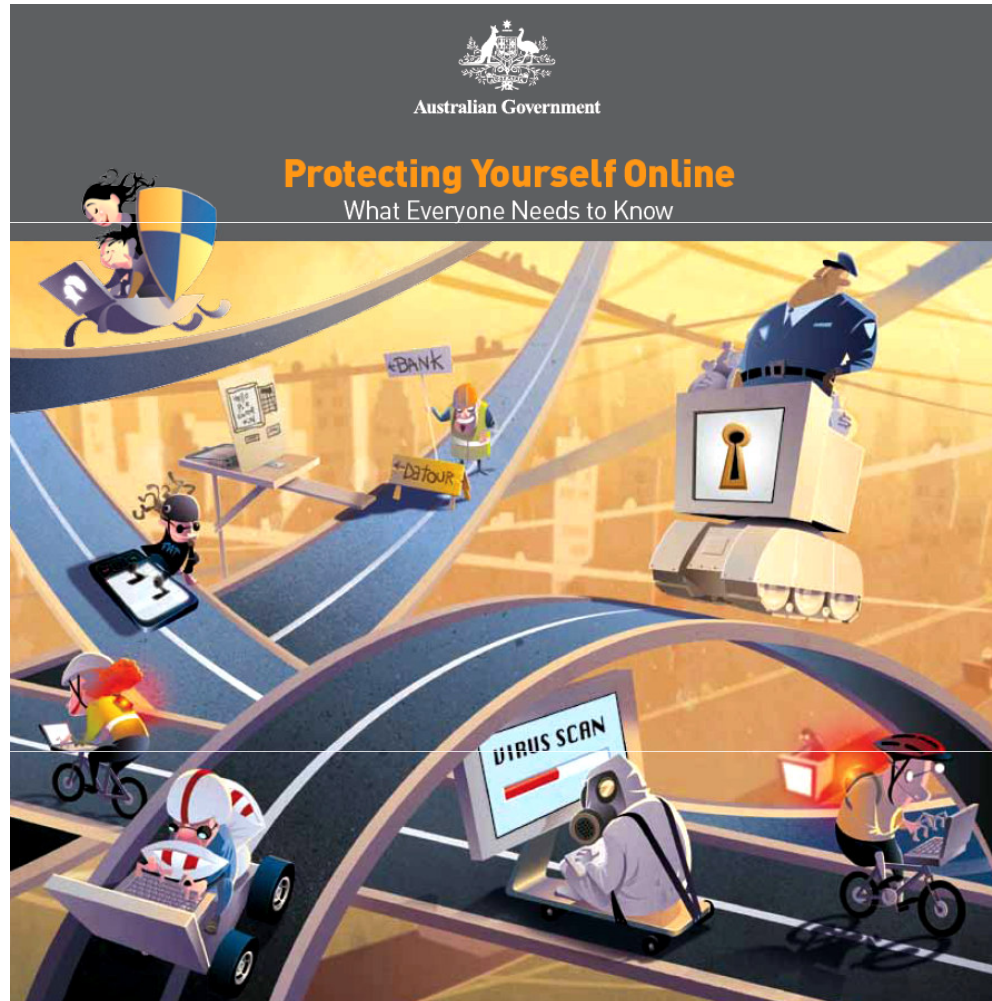


University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world



University of Technology,  
Jamaica

**ITU Centres of Excellence Network for the Caribbean Region**  
**Developing a National and Organizational Cybersecurity Strategy**  
*13-15 September, Kingston, Jamaica*


**International  
Telecommunication  
Union**

*Committed to connecting the world*



# Malaysian Government: MOSTi





# Malaysia: Cybersecurity Strategy

## The Eight Policy Thrusts

### **THRUST 1: Effective Governance**

Centralise coordination of national cyber security initiatives  
Promote effective cooperation between public and private sectors  
Establish formal and encourage informal information sharing exchanges

### **THRUST 2: Legislative & Regulatory Framework**

Review and enhance Malaysia's cyber laws to address the dynamic nature of cyber security threats  
Establish progressive capacity building programmes for national law enforcement agencies  
Ensure that all applicable local legislation is complementary to and in harmony with international laws, treaties and conventions

### **THRUST 3: Cyber Security Technology Framework**

Develop a national cyber security technology framework that specifies cyber security requirement controls and baselines for CNII elements  
Implement an evaluation/certification programme for cyber security product and systems

### **THRUST 4: Culture of security and Capacity Building**

Develop, foster and maintain a national culture of security  
Standardise and coordinate cyber security awareness and education programmes across all elements of the CNII  
Establish an effective mechanism for cyber security knowledge dissemination at the national level  
Identify minimum requirements and qualifications for information security professionals

### **THRUST 5: Research & Development Towards Self-Reliance**

Formalise the coordination and prioritization of cyber security research and development activities  
Enlarge and strengthen the cyber security research community  
Promote the development and commercialization of intellectual properties, technologies and innovations through focused research and development  
Nurture the growth of cyber security industry

### **THRUST 6: Compliance and Enforcement**

Standardise cyber security systems across all elements of the CNII  
Strengthen the monitoring and enforcement of standards  
Develop a standard cyber security risk assessment framework

### **THRUST 7: Cyber Security Emergency Readiness**

Strengthen the national computer emergency response teams (CERTs)  
Develop effective cyber security incident reporting mechanisms  
Encourage all elements of the CNII to monitor cyber security events  
Develop a standard business continuity management framework  
Disseminate vulnerability advisories and threat warnings in timely manner  
Encourage all elements of the CNII to perform periodic vulnerability assessment programmes

### **THRUST 8: International Cooperation**

Encourage active participation in all relevant international cyber security bodies, panels and multi-national agencies  
Promote active participation in all relevant international cyber security by hosting an annual international cyber security conference

© Ministry of Science, Technology And Innovation



University of Technology,  
Jamaica

**ITU Centres of Excellence Network for the Caribbean Region**  
**Developing a National and Organizational Cybersecurity Strategy**  
13-15 September, Kingston, Jamaica



**International  
Telecommunication  
Union**

**Committed to connecting the world**

# Cybersecurity Agency: Case Studies

- Common roles and responsibilities of these national cyber agencies:
  - *Cyber Alerts:* Management of the National Response to Cyber Alerts, and Major Attacks
  - *Education:* Co-ordination of the National Awareness and Skills Training Programmes
  - *Laws:* Leadership role in the development and approval of new cyber legislation
  - *Cybercrime:* Facilitation for the establishment of a National Cybercrime or e-Crime Unit
  - *Standards:* Setting the national cybersecurity standards and auditing compliance
  - *International:* Leadership in the promotion of international partnerships for cybersecurity
  - *Research:* Support for research & development into cybersecurity technologies & solutions
  - *Critical Sectors:* Co-ordination of National Programmes for Critical Information Infrastructure

*.....Next we'll flow chart the typical process and strategic decisions required to establish a National Cybersecurity Agency (NCA) in a country such as Jamaica*



# **\* Workshop Session 9 \***

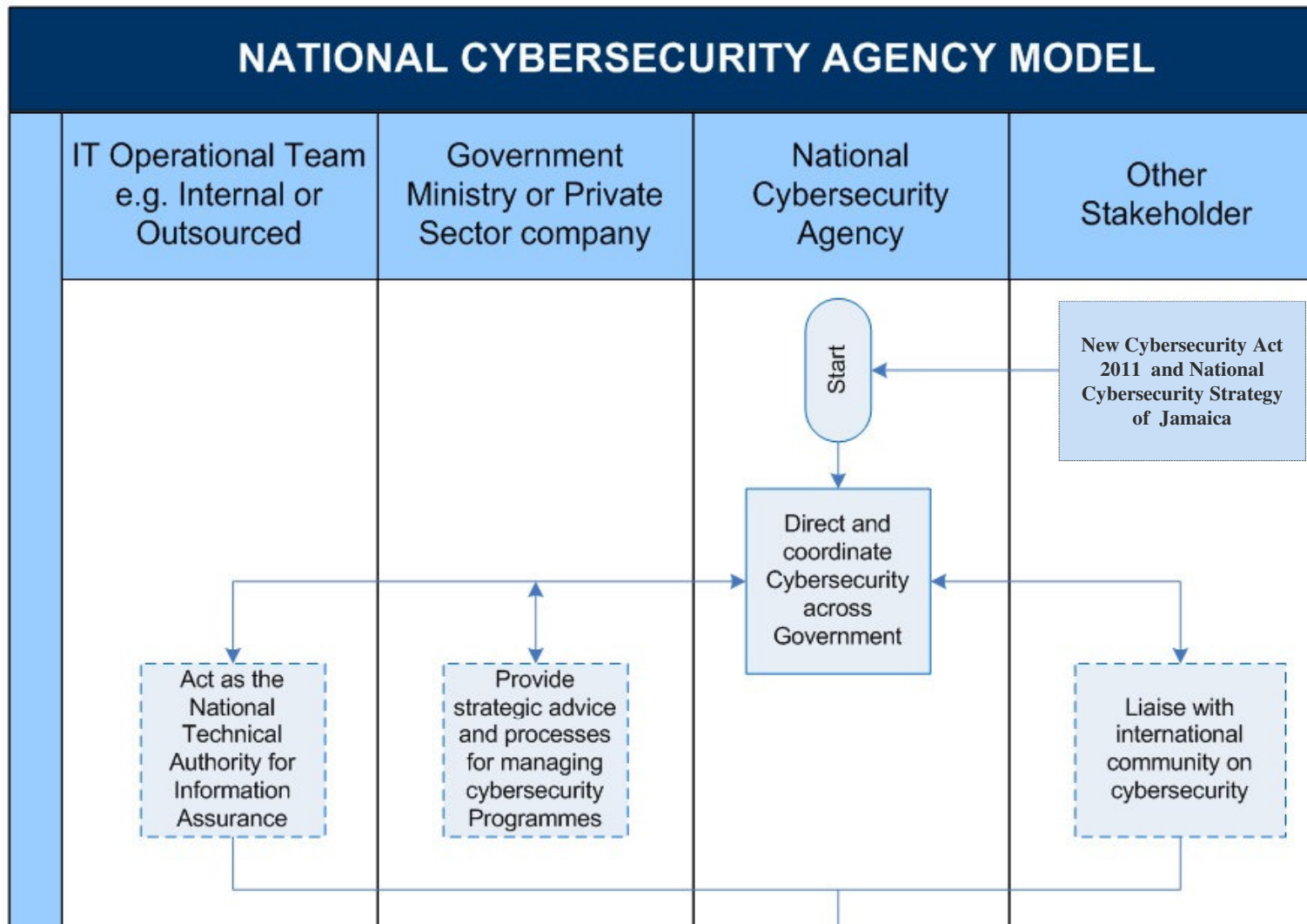
## **ITU Global Cybersecurity Agenda:**

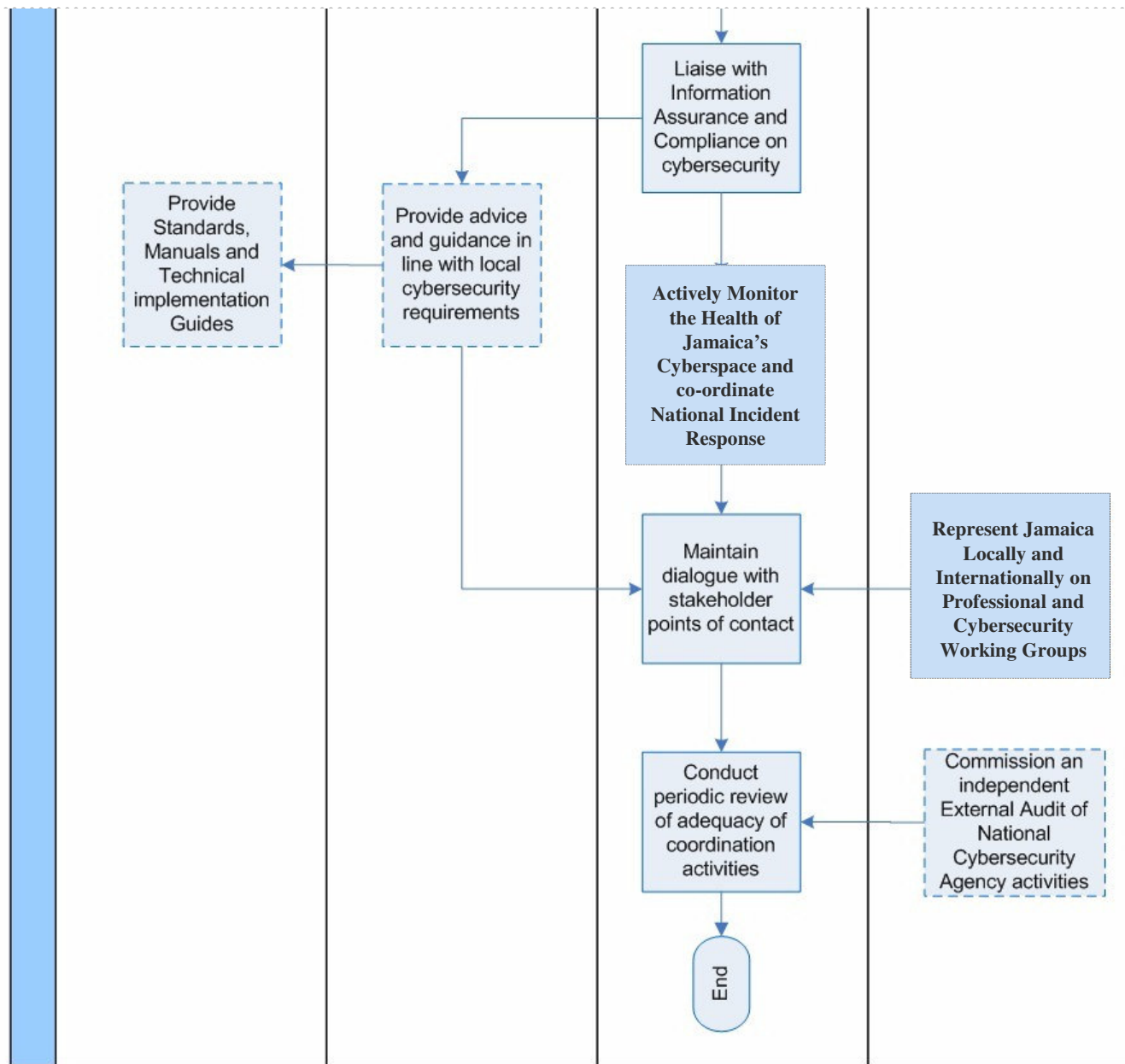
### ***...Operational Risks and Organisational Structures***

<b>1 – Structures and Strategies</b>	<b>2 - Cybersecurity Co-ordination</b>	<b>3 – National Cyber Agency</b>
<b>4 – Cyber Agency Case Studies</b>	<b>5 – Models for Cyber Agencies</b>	<b>6 – National Roll-Out Plans</b>
<b>7 – Emergency Response - CERT</b>	<b>8 – National Cybercrime Unit</b>	<b>9 – Benefits for Jamaica</b>



# Proposed Model for the National Cybersecurity Agency of Jamaica





# \* Workshop Session 9 \*

## ITU Global Cybersecurity Agenda:

### *...Operational Risks and Organisational Structures*

1 – Structures and Strategies	2 - Cybersecurity Co-ordination	3 – National Cyber Agency
4 – Cyber Agency Case Studies	5 – Models for Cyber Agencies	6 – National Roll-Out Plans
7 – Emergency Response - CERT	8 – National Cybercrime Unit	9 – Benefits for Jamaica





# National Cyber Roll-Out Plans

- Once the National Cybersecurity is established, the action plans will need to be agreed, prioritise and road mapped, and then rolled-out during the course of 12 to 24 months:
  - *Phase 1* : Central Government Ministries and Agencies – Upgrade ICT Systems and ensure that all staff are fully “cyber aware” and trained to their operational needs
  - *Phase 2* : Critical Service Sectors – Work with the ICT & business leaders within each of the target sectors such as Telecomms, Banking, Transport & Energy to ensure that their ICT and business operations are upgraded to agreed national standards
  - *Phase 3* : Establish specialised organisations including the National CERT for Incident Management, and the National Cybercrime Unit in partnership with the Police Authorities
  - *Phase 4* : Regional Government Administrations and Local Offices – Ensure that the ICT Networks, Applications and Databases are secure, and that staff are “cyber aware”
  - *Phase 5* : Small & Medium Enterprises (SMEs) – Ensure that the smaller business operations are also fully aware of the importance of information security and they have access to government certified cybersecurity training courses for their business needs

*...Next we'll consider the organisation of the CERT & e-Crime Unit in more detail.*



# **\* Workshop Session 9 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Operational Risks and Organisational Structures***

<b>1 – Structures and Strategies</b>	<b>2 - Cybersecurity Co-ordination</b>	<b>3 – National Cyber Agency</b>
<b>4 – Cyber Agency Case Studies</b>	<b>5 – Models for Cyber Agencies</b>	<b>6 – National Roll-Out Plans</b>
<b>7 – Emergency Response - CERT</b>	<b>8 – National Cybercrime Unit</b>	<b>9 – Benefits for Jamaica</b>






# Emergency Response - CERTs

- The provision of a CERT (Computer Emergency Response Centre) or CSIRT (Computer Security Incident Response Team) will be a early top priority for any newly established National Cybersecurity Organisation. In many countries the "Education Sector" will already have built some form of CERT for their own needs.
- There are many excellent on-line guides to the establishment of a CERT or CSIRT such as "Organizational Models for CSIRTs" - Published by Carnegie Mellon University. Many such useful documents can be downloaded from [www.cert.org](http://www.cert.org)
- The European Agency – ENISA – is also an excellent source for the latest research and guides to the installation and management of national CERTs/CSIRTs
- Practically all the operational CERTs are members of a much wider international CERT community that shares information regarding the latest cyber incidents, alerts, malicious attacks & hackers. They will often work together to identify the source of international cyberattacks, and hence to counter major cyberthreats

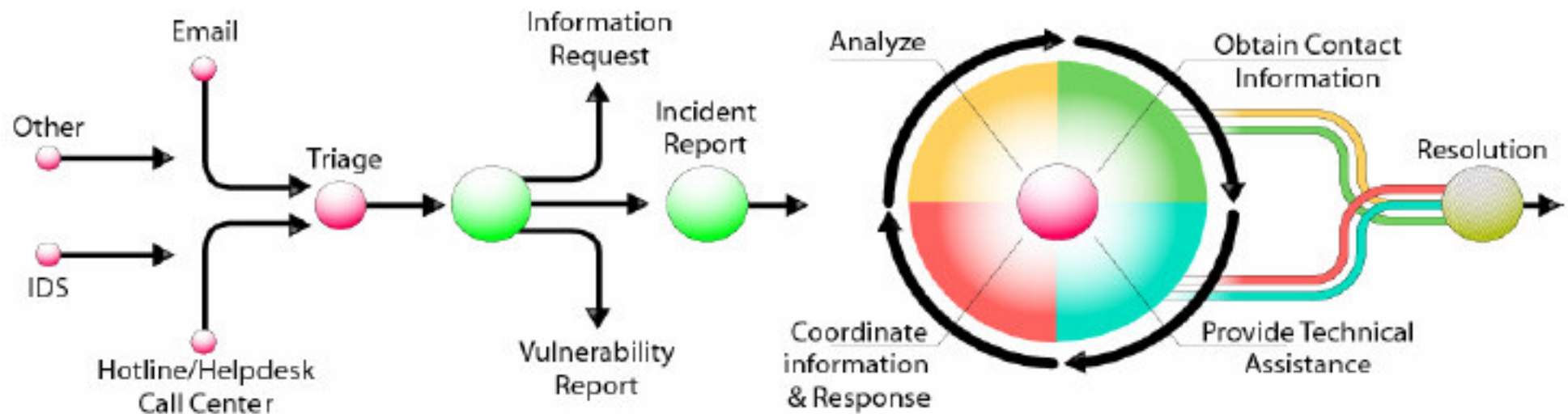


# Typical CERT/CSIRT Services

Reactive Services 	Proactive Services 	Security Quality Management Services 
<ul style="list-style-type: none"> <li>+ Alerts and Warnings</li> <li>+ Incident Handling                             <ul style="list-style-type: none"> <li>– Incident analysis</li> <li>– Incident response on site</li> <li>– Incident response support</li> <li>– Incident response coordination</li> </ul> </li> <li>+ Vulnerability Handling                             <ul style="list-style-type: none"> <li>– Vulnerability analysis</li> <li>– Vulnerability response</li> <li>– Vulnerability response coordination</li> </ul> </li> <li>+ Artifact Handling                             <ul style="list-style-type: none"> <li>– Artifact analysis</li> <li>– Artifact response</li> <li>– Artifact response coordination</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>○ Announcements</li> <li>○ Technology Watch</li> <li>○ Security Audit or Assessments</li> <li>○ Configuration &amp; Maintenance of Security Tools, Applications, &amp; Infrastructures</li> <li>○ Development of Security Tools</li> <li>○ Intrusion Detection Services</li> <li>○ Security-Related Information Dissemination</li> </ul>	<ul style="list-style-type: none"> <li>✓ Risk Analysis</li> <li>✓ Business Continuity &amp; Disaster Recovery Planning</li> <li>✓ Security Consulting</li> <li>✓ Awareness Building</li> <li>✓ Education/Training</li> <li>✓ Product Evaluation or Certification</li> </ul>

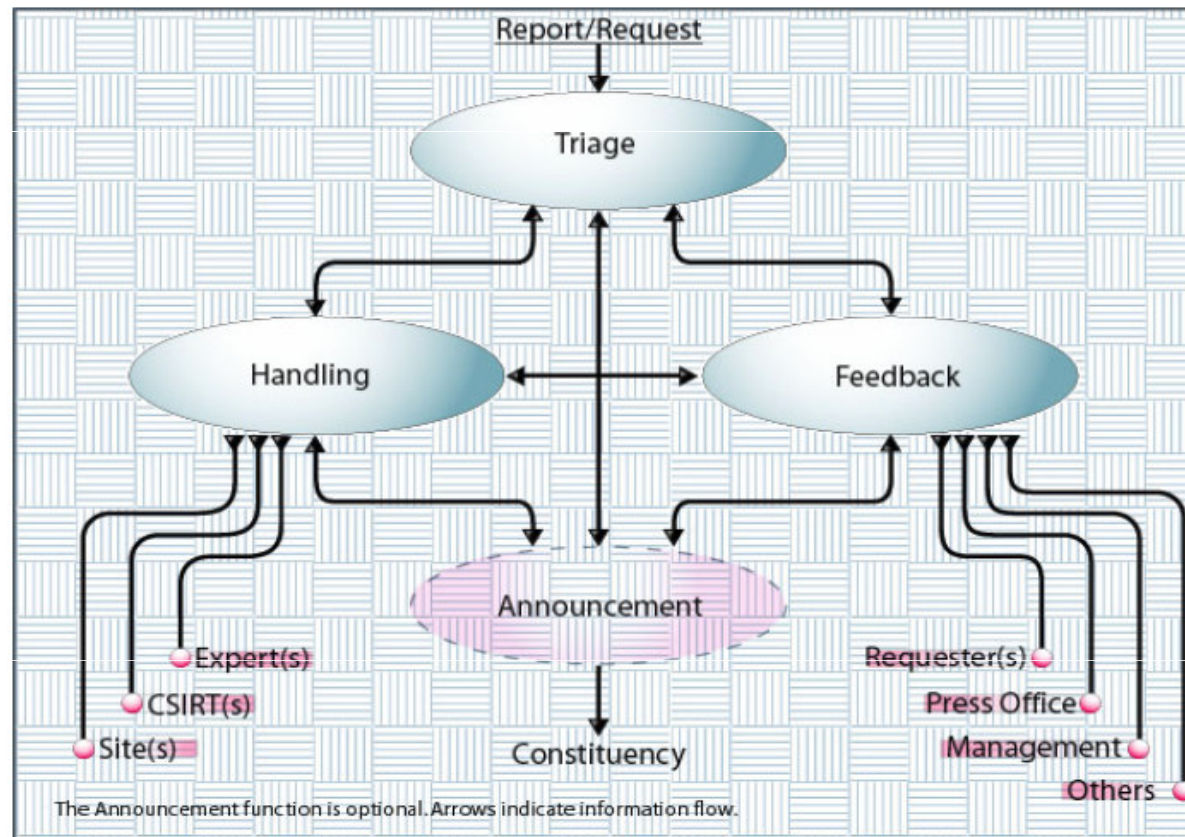


# Incident Handling Life-Cycle





# CERT/CSIRT: Incident Handling Service Functions





# **\* Workshop Session 9 \***

## **ITU Global Cybersecurity Agenda:**

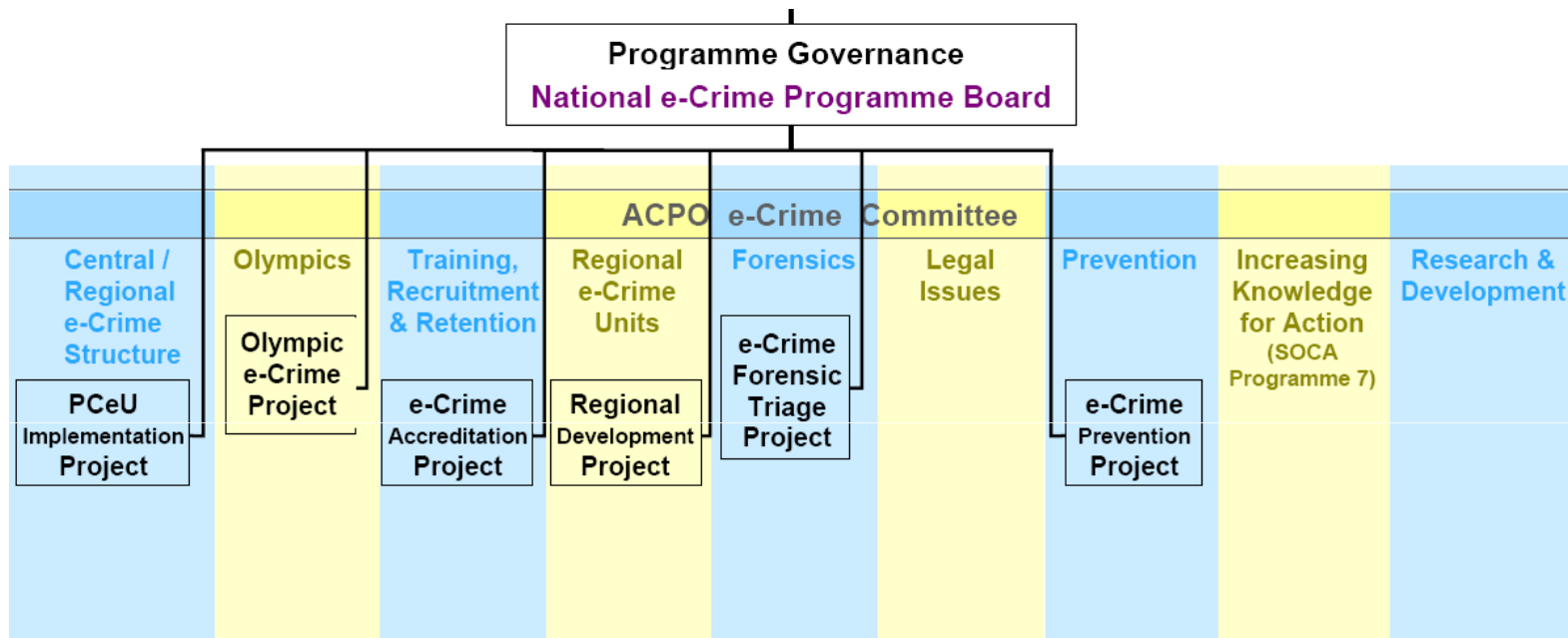
### ***...Operational Risks and Organisational Structures***

<b>1 – Structures and Strategies</b>	<b>2 - Cybersecurity Co-ordination</b>	<b>3 – National Cyber Agency</b>
<b>4 – Cyber Agency Case Studies</b>	<b>5 – Models for Cyber Agencies</b>	<b>6 – National Roll-Out Plans</b>
<b>7 – Emergency Response - CERT</b>	<b>8 – National Cybercrime Unit</b>	<b>9 – Benefits for Jamaica</b>

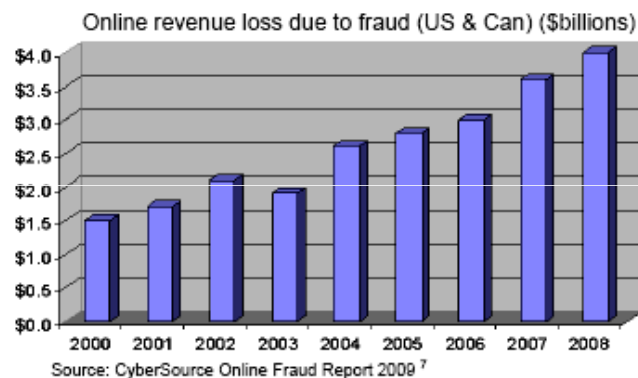
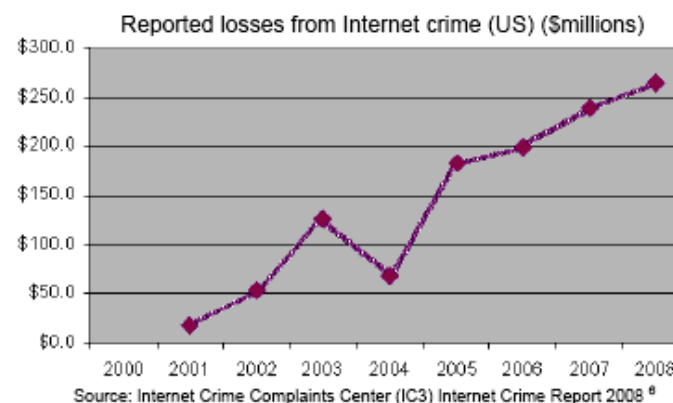
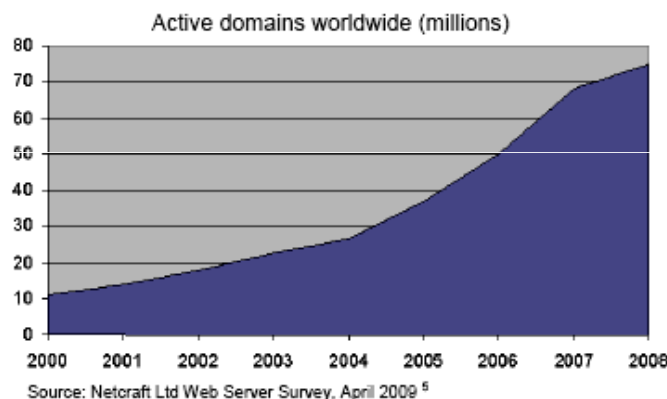


# National Cybercrime Unit

- We'll use the UK e-Crime Unit as our Case Study for "Best Practice". This Unit is established under the Association of Chief Police Officers (ACPO) with useful documentation regarding its strategic goals, organisation & guidelines available here: [www.met.police.uk/pceu/](http://www.met.police.uk/pceu/)



# Annual Growth in Cybercrime



# E-Crime Unit : Electronic Evidence Guide



## Good Practice Guide for Computer-Based Electronic Evidence

Official release version

...We'll be considering the Technological Aspects of Cybercrime such as Digital Forensics in our 2<sup>nd</sup> Workshop – 16<sup>th</sup>/17<sup>th</sup> Sept



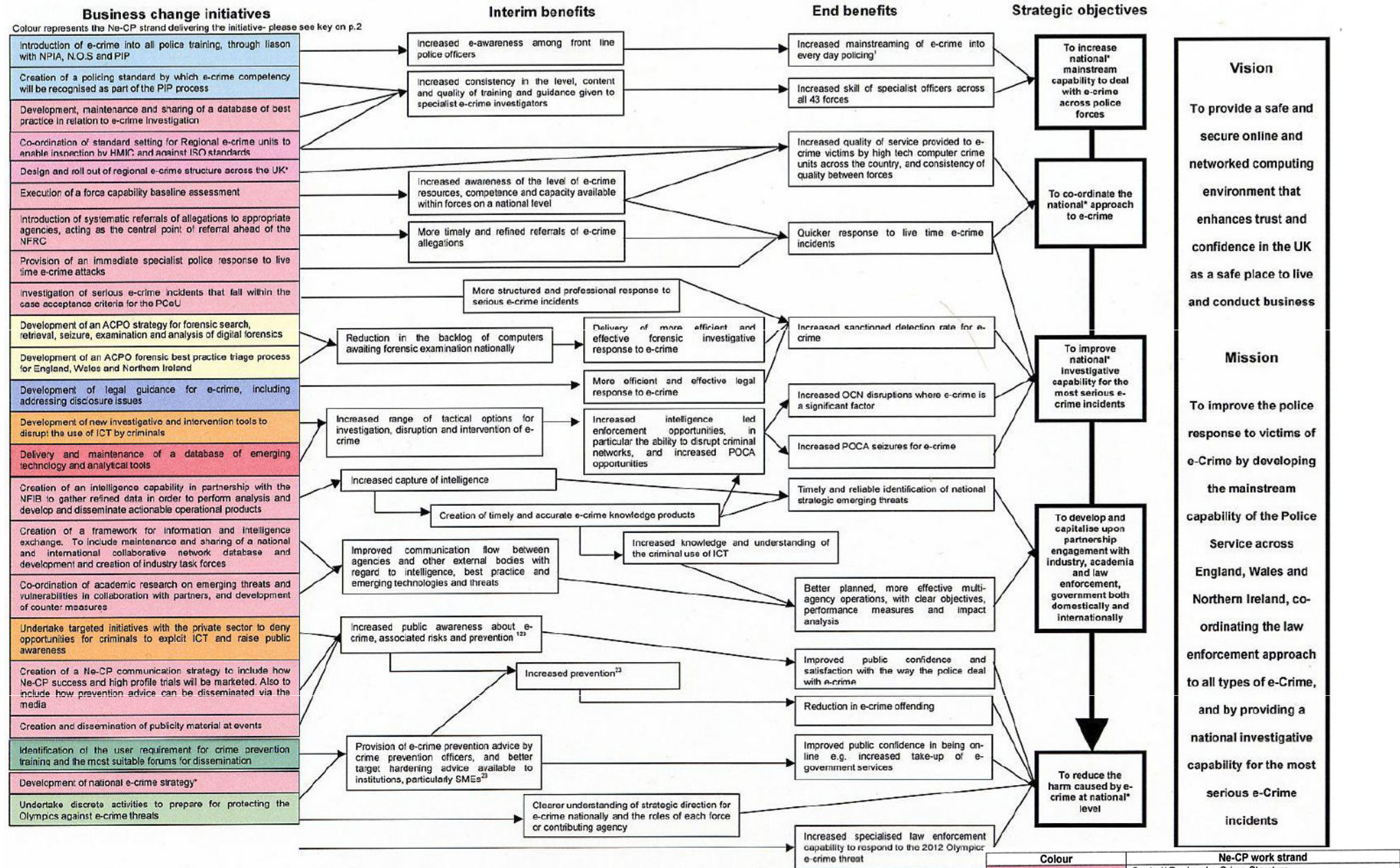
University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world







# e-Crime Organisation: Virtual Task Force

- The UK e-Crime Unit was established through a virtual taskforce between the police, industry and academia. This included critical UK sectors such as banking, telecomms, and Internet Service Providers.



Jamaica : JCF – OCID – *“Jamaican Constabulary Force – Organised Crime Investigative Division”*



# "Harm" Impact Framework: UK e-Crime (1)

	Individual (I)	Community/ Region (C)	UK/ International (U)
<b>Physical (harm to the person or property)</b>  <b>1</b>	a. Physical and mental harm caused to individuals by the occurrence of traditional crimes enabled by computers e.g. harms to the individual caused by drug dealing/ kidnap/ theft b. Physical harm caused by changing the configuration or damaging the hardware or software of victim's computers c. Stress, and its physical effects, triggered by serious incidents such as theft of credit history and identity fraud. Risk of suicide. d. Emotional distress caused by lower tier offences such as phishing/ spam email	a. Physical or mental harm to individuals of a particular demographic group (e.g. young or old) or within a particular community or geographical area caused by traditional crimes enabled by computers b. Physical or mental harm to individuals within a particular community or geographical area caused by criminal activity funded from the proceeds of e-crime (drug related deaths, sexually exploited human trafficking victims) c. Physical harm caused by changing the configuration or damaging the hardware or software of computer networks i.e. an individual company's or government department's computer system	a. Physical or mental harm to individuals within the UK caused by traditional crimes enabled by computers b. Physical or mental harm to individuals within the UK caused by criminal activity funded from the proceeds of e-crime (drug related deaths, sexually exploited human trafficking victims) c. Physical harm caused by changing the configuration or damaging the hardware or software of national or international computer networks i.e. the government secure network
<b>Social (harm to the social environment e.g. crime levels)</b>  <b>2</b>	a. Loss or harm to an individual's trust in the online community and in the capability of law enforcement agencies to bring the perpetrators of e-crime to justice b. Increased difficulty and opportunity cost of the increased time taken for individuals to complete administrative procedures online, such as applying for a credit card c. Spiralling effect of involvement in e-crime on the individual i.e. as a stepping stone crime type	a. Damage to the sense of "well- being" of particular online communities such as the banking community, social community (Facebook) and a widespread loss of faith in the ability of these online communities to protect information b. Damage to the sense of "well being" of communities as online services and the Internet are perceived to be dominated by seemingly "untouchable" criminal elements, or by corrupted business leaders from the technology sector	a. Destruction of the world wide web and collapse of the online community b. Damage to Immigration computer systems causing porous borders and allowing international criminals to move between countries undetected
<b>Environmental (harm to the physical environment e.g. parks)</b>  <b>3</b>	a. Emotional distress and inconvenience to individuals if utility supply is limited or withdrawn b. Risk of physical harm to individuals by contamination of resources c. Impact to the service providers who are unable to meet supply demands due to attack	a. Loss of confidence in the supply of essential services to the community. b. Damage to the reputation of private and public sector suppliers such as National Health Service, Schools and Public Transport c. Individuals and communities isolated by loss of communication and trust in the delivery of everyday services	a. Decrease in potential government investment in outdoor and other communal areas etc caused by a decrease in revenue from overseas investors in the UK. This would be caused by the reputation of the UK as the 2 <sup>nd</sup> country most likely to lose or compromise data online



# "Harm" Impact Framework: UK e-Crime (2)

<b>Economic (monetary cost to individuals, industry, countries)</b>  4	a. Financial loss to individuals due to online theft from bank accounts b. Increased insurance premiums charged to individuals to cover banks' losses c. Cost of repairing or replacing physical damage caused to an individual's computer, hardware or software d. Delays in the payment of benefits and other state allowances to individuals e. Anxiety to individuals caused by the difficult financial climate and the incentive this provides for increased levels of e-crime	a. Economic impact on the business community as a result of losses from fraud or online theft and a decrease in trade b. Regional impact of increased bank costs could include lower salaries and unemployment	a. Loss of interest revenue as a result of taxes collected late by HMRC will impact on the money available to pay towards national services such as the NHS b. Loss of government data c. Shock to the stability of the UK banking system may impact internationally and will affect UK and international revenue d. Opportunity cost of government investment in the law enforcement response to e-crime
<b>Structural/ Infrastructure (harm to processes and mechanisms)</b>  5	a. Damage to the individual's perceptions of new technology i.e. banking internet services, due to the perceived risk of online fraud b. Individual's loss of faith in the ability of public/ private bodies to protect them/ their property from the threat and consequences of e-crime	a. Damage to companies' and communities' perceptions of new technology b. Sector, community or group's loss of faith in the ability of public/ private bodies to protect them/ their property from the threat and consequences of e-crime	a. Damage to national infrastructure e.g. road system, payments system, health records, criminal records b. State sponsored attacks on national infrastructure
<b>Reputation/ Credibility (harm to the reputation of individuals, communities and countries)</b> 6	a. Individual users' loss of faith in online services and the companies behind these services b. Damage to individual's reputation and credibility caused by theft of identity or by online defamation	a. Loss of business revenue caused by a decrease in credibility in online services	a. Loss or decrease in the UK's gross domestic product as a result of decreased trade online caused by a loss of credibility in online trading and services b. Damage to the government's, Royalty's or the UK's credibility caused by defacement of major websites

**Impacts: (1) Physical; (2) Social; (3) Environmental; (4) Economic; (5) Structural; (6) Reputation;**



# **\* Workshop Session 9 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Operational Risks and Organisational Structures***

<b>1 – Structures and Strategies</b>	<b>2 - Cybersecurity Co-ordination</b>	<b>3 – National Cyber Agency</b>
<b>4 – Cyber Agency Case Studies</b>	<b>5 – Models for Cyber Agencies</b>	<b>6 – National Roll-Out Plans</b>
<b>7 – Emergency Response - CERT</b>	<b>8 – National Cybercrime Unit</b>	<b>9 – Benefits for Jamaica</b>



# Economic Benefits for Jamaica

- The implementation of a National Cybersecurity Agency, CERT and e-Crime Unit would have significant economic benefits for Jamaica:

- 1) Boosted trust in the security of the Jamaican Banking and Financial Sector
- 2) Reduced incidence and impact of cyberattacks & cyberterrorism on critical sectors
- 3) Increased travel and tourism to the hotels and resorts due to increased total security
- 4) Improved security for import/export trade at ports including agricultural products
- 5) Management of national and international cybercrime through the e-Crime Unit
- 6) Quick response by the CERT/CSIRT to cyber alerts and major ICT incidents
- 7) Improved position for Jamaica as Regional eTrading Hub for eCommerce Services
- 8) Potential for cybersecurity R&D to result in Entrepreneurial Business Ventures
- 9) Greater trust in Jamaican Government eServices by Citizens and Businesses

*...In summary, the development of national and enterprise cybersecurity constitutes and business proposition in which there may be significant payoff for Jamaica in future years for investments in the proposed national cybersecurity action plan and roadmap!*



#	Item	CYBERSECURITY FRAMEWORK POLICY GOALS
1	<b>Information Security Policy</b>	A Ministry or Agency's security policy should flow from the National Cybersecurity Strategy. The policy demonstrates management's support for, and commitment to information security across their organisation.
2	<b>Organisation of Information Security</b>	A management framework initiates and controls the implementation of information security within a Ministry or Agency. The main activities include: <ul style="list-style-type: none"> <li>Defining and maintaining cybersecurity roles and responsibilities; and</li> <li>Operating security management committee and working groups.</li> </ul>
3	<b>Asset Management</b>	Ministries or Agencies should have processes for maintaining appropriate protection of assets. For example, they should have an information classification scheme to define an appropriate set of protection levels & communicate the need for special handling measures.
4	<b>Human Resources Security i.e. Staff Vetting and Clearance)</b>	Among other things, best human resources security practice requires the vetting of all employees, contractors and third party users accessing classified information to reduce the risk of theft, fraud or misuse of facilities.
5	<b>Physical and Environmental Security</b>	Ministries or Agencies should ensure that critical or sensitive information processing facilities reside in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls.
6	<b>Communications and Operations Management</b>	Ministries or Agencies should establish responsibilities and procedures for the management and operation of all information processing facilities. For example, they should enforce appropriate segregation of duties to reduce the risk of negligent or deliberate system misuse.
7	<b>Access Control</b>	Ministries or Agencies should only grant access to information, information processing facilities, and business processes based on business & security requirements. Access control rules should also take account of policies for information dissemination & authorisation.
8	<b>Information systems acquisition, development and maintenance</b>	Ministries or Agencies should identify and agree security requirements prior to the development and info systems implementation.
9	<b>Information security incident management</b>	Ministries or Agencies should design processes to ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
10	<b>Business Continuity Management</b>	Ministries or Agencies should undertake Business Continuity Planning to counteract interruptions to activities, to protect critical processes from major system failures or disasters and to ensure their timely resumption.
11	<b>Compliance</b>	Ministries or Agencies should adopt compliance-checking frameworks to avoid breaches of any law, regulatory or contractual obligations, and of any security requirements.

# \* ITU Cybersecurity Strategy \*

## "3-Day Workshop Overview"

<b>S1- Mon: 9:30-11:00</b>  <b>"The Cybersecurity Challenge!..."</b>	<b>S2-Mon: 11:30-13:00</b>  <b>"The Need for Action!"</b>	<b>S3 - Mon:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Cybersecurity Action Plans"</b>	<b>S4 - Mon:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Cybersecurity Action Plans"</b>
<b>S5- Tues: 9:30-11:00</b>  <b>ITU Cyber Agenda: 1</b> <b>"Cybercrime and Legislation"</b>	<b>S6-Tues: 11:30-13:00</b>  <b>ITU Cyber Agenda: 2</b> <b>"Technological Risks and Solutions"</b>	<b>S7 -Tues:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Legislation and Regulations"</b>	<b>S8 -Tues:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Legislation and Regulations"</b>
<b>S9- Wed: 9:30-11:00</b>  <b>ITU Cyber Agenda: 3</b> <b>"Operational Risks and Organisational Structures"</b>	<b>S10-Wed:11:30-13:00</b>  <b>ITU Cyber Agenda: 4&amp;5</b> <b>"Capacity Building and Collaboration"</b>	<b>S11-Wed:14:00-15:30</b> <b>Group Session:</b>  <b>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</b>	<b>S12-Wed:16:00-17:30</b> <b>Group Session:</b>  <b>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</b>





# **\* Workshop Session 10 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Cybersecurity Capacity Building and International Collaboration & Resources***

<b>1 – Aim: Cyber Skills Building</b>	<b>2 – National Cyber Framework</b>	<b>3 – Cybersecurity Skill Needs</b>
<b>4 – Cyber Skills Certification</b>	<b>5 – Training &amp; Awareness</b>	<b>6 – Public-Private Partnerships</b>
<b>7 – International Collaboration</b>	<b>8 – Next Steps for Jamaica</b>	<b>9 – On-Line Cyber Resources</b>



# **\* Workshop Session 10 \***

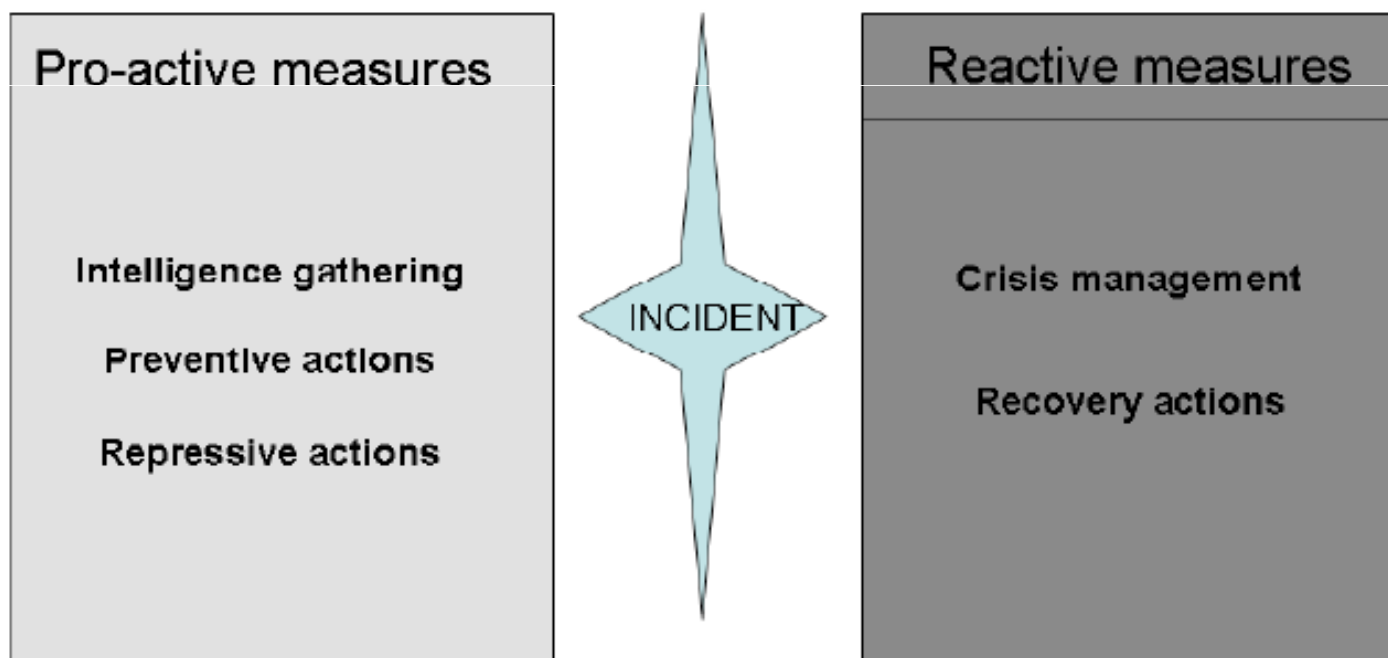
## **ITU Global Cybersecurity Agenda:**

### ***...Cybersecurity Capacity Building and International Collaboration & Resources***

<b>1 – Aim: Cyber Skills Building</b>	<b>2 – National Cyber Framework</b>	<b>3 – Cybersecurity Skill Needs</b>
<b>4 – Cyber Skills Certification</b>	<b>5 – Training &amp; Awareness</b>	<b>6 – Public-Private Partnerships</b>
<b>7 – International Collaboration</b>	<b>8 – Next Steps for Jamaica</b>	<b>9 – On-Line Cyber Resources</b>



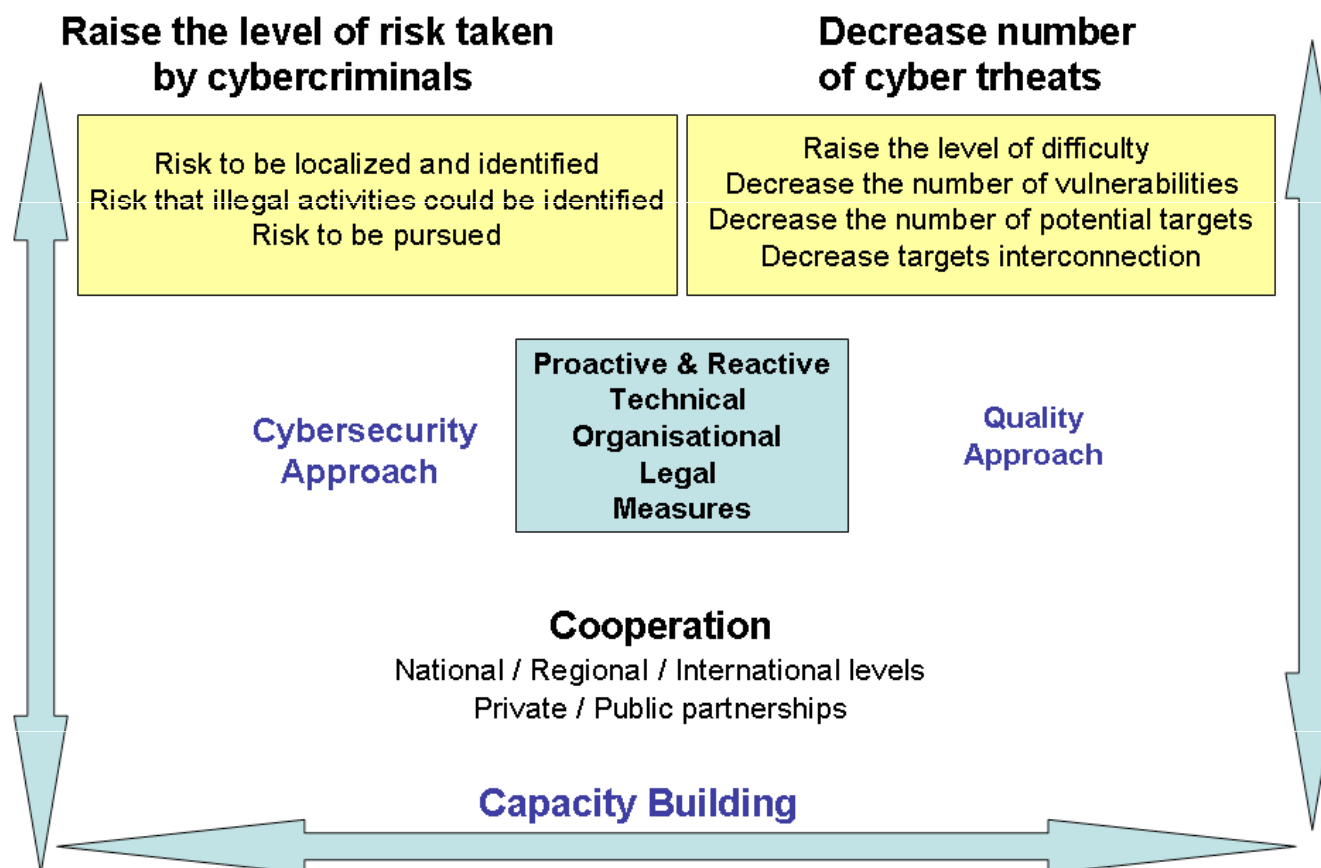
# Generic Cybersecurity Functions



Report to the ITU – High Level Expert Group - 20098



# Cybersecurity Capacity Building



# Cyber Skills & Capacity Building

- Professional Cybersecurity Skills are currently in extremely short supply even in developed countries & regions such as USA, UK and Europe!

## A Human Capital Crisis in Cybersecurity

### Technical Proficiency Matters

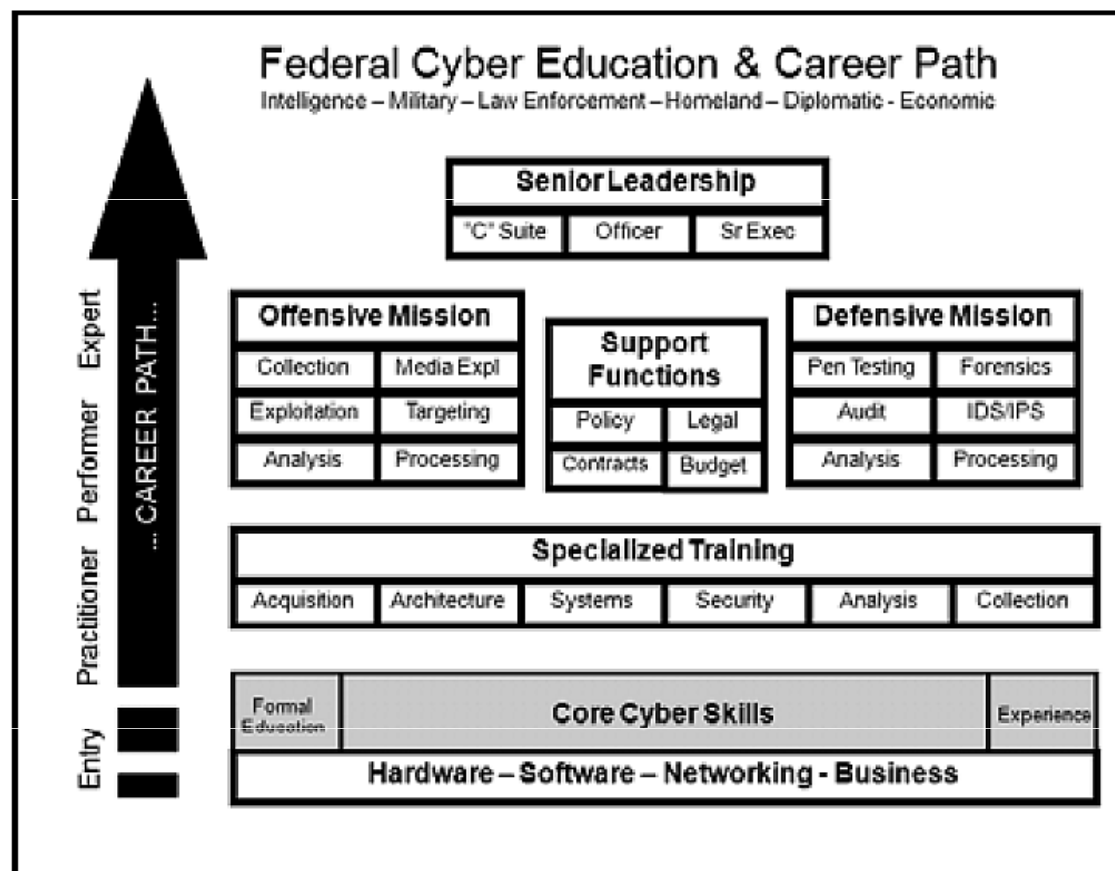
A White Paper of the  
CSIS Commission on Cybersecurity for the 44th Presidency

- The US Centre for Strategic and International Studies published a report in July 2010 recommending ways to overcome the skills crisis



- The UK Government launched the Cybersecurity Challenge – July 2010

# Cyber Education & Career Path



**CSIS** | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



# Some Key Cybersecurity Roles

- 1) Chief Information Security Officer (CSO/CISO)
- 2) Systems Operations & Maintenance Personnel
- 3) Network Security Specialists
- 4) Digital Forensics & Incident Response Analysts
- 5) Information Security Assessor
- 6) Information Systems Security Officer
- 7) Security Architect
- 8) Vulnerability Analyst
- 9) Information Security Systems & Software Development



# Cybersecurity Roles: Job Specs (1)

**1. Chief Information Security Officer-** The Chief Information Security Officer (CISO) is responsible for the information security strategy within an organization. The CISO establishes, implements, and monitors the development and subsequent enforcement of the organization's information security program (i.e., policies, procedures, security architecture standards, security awareness and training program, IT contingency plans, IT security compliance issues). The CISO leads the evaluation and assessment of the security program to ensure that all aspects are in compliance with security requirements, while understanding security threats and vulnerabilities to operations and the organization's environment. The CISO is responsible for information security risk management (e.g., determines risk impact, establishes risk mitigation plans and programs, works with business owners to devise processes for risk assessment) within the organization. The CISO manages the incidents response program (e.g., identifies, reports, and remediates incidents).

**2. Systems Operations & Maintenance Professional-** The Systems Operations and Maintenance Professional supports and implements the security of information and information systems during the operations, maintenance, and enhancements phases of the systems development life cycle. The Systems Operations and Maintenance Professional is also responsible for implementing server configurations, operating systems, database systems, firewalls, patch management, and account management to protect the systems against threats and vulnerabilities.

**3. Network Security Specialist-** The Network Security Specialist is responsible for examining malicious software, suspicious network activities, and non-authorized presence in the network to analyze the nature of the threat, and secure and monitor firewall configurations. The Network Security Specialist needs to understand the specimen's attack capabilities, its propagation characteristics, and define signatures for detecting malware presence.

**4. Digital Forensics & Incident Response Analyst-** The Digital Forensics and Incident Response Analyst performs a variety of highly technical analyses and procedures dealing with the collection, processing, preservation, analysis, and presentation of computer-related evidence, and is responsible for disseminating and reporting cyber-related activities, conducting vulnerability analyses and risk management of computer systems and all applications during all phases of the systems development lifecycle. The Digital Forensics and Incident Response Analyst provides oversight of incident data flow and response, content, and remediation, and partners with other incident response centers in maintaining an understanding of threats, vulnerabilities, and exploits that could impact networks and assets.



# Cybersecurity Roles: Job Specs (2)

**5. Information Security Assessor-** The Information Security Assessor is responsible for overseeing, evaluating, and supporting compliance issues pertinent to the organization. Individuals in this role perform a variety of activities that encompass compliance from internal and external perspectives. These include leading and conducting internal investigations, helping employees to comply with internal policies and procedures, and serving as a resource for external compliance officers during independent assessments. The Information Security Assessor provides guidance and autonomous evaluation of the organization to management. This individual is responsible for planning and executing information systems operational assessment by obtaining, analyzing, and appraising competent evidential data for forming an objective opinion on the adequacy of information systems, procedures, and documentation. This individual also prepares, tests, and utilizes generalized computer audit software, programs, and questionnaires for accomplishing audit objectives and procedures.

**6. Information Systems Security Officer-** The Information Systems Security Officer (ISSO) specializes in the information and security strategy within a system and is engaged throughout the systems development life cycle. The ISSO is charged with the development and subsequent enforcement of the company's security policies and procedures, security awareness programs, business continuity and disaster recovery plans, and all industry and governmental compliance issues. The ISSO communicates with the business at the system level and understands security threats and vulnerabilities to the operations and the system's environment.

**7. Security Architect-** The Security Architect is responsible for implementing business needs. The Security Architect supports the business function as well as technology and environmental conditions (e.g., law and regulation), and translates them into security designs that support the organization to efficiently carry out its activities while minimizing risks from security threats and vulnerabilities.

**8. Vulnerability Analyst-** The Vulnerability Analyst is responsible for detecting threats and vulnerabilities in target systems, networks, and applications by conducting systems, network, and web penetration testing. The Vulnerability Analyst identifies flaws that can be exploited to cause business risk, and provides crucial insights into the most pressing issues, suggesting how to prioritize security resources.

**9. Information Security Systems & Software Development Specialist\*\*-** The Information Security Systems and Software Development Specialist is responsible for secure design, development, testing, integration, implementation, maintenance, and/or documentation of software applications (web based and non-web) following formal secure systems development lifecycle processes and using security engineering principles.



# INFORMATION SECURITY WORKFORCE DEVELOPMENT MATRIX\*

<b>Systems Operations and Maintenance Professional**:</b> The Systems Operations and Maintenance Professional supports and implements the security of information and information systems during the operations, maintenance, and enhancements phases of the systems development life cycle. The Systems Operations and Maintenance Professional is also responsible for implementing server configurations, operating systems, database systems, firewalls, patch management, and account management to protect the systems against threats and vulnerabilities.				
Performance Level	Description/Complexity	Competencies/Skills	Suggested Credentials	Suggested Learning & Development Sources
<b>I: Entry</b>	<p>Has a basic understanding of computer systems and related information security software and hardware components</p> <p>Ability to perform basic security system administration duties including software and hardware installation, troubleshooting, system backup, network component maintenance</p> <p>Basic understanding of tools and methods for identifying anomalies in system behavior; develops ability to recognize anomalies</p> <p>Applies skills and abilities with supervision on projects, programs, and initiatives with low threat and scope (e.g., inter-office)</p>	<p>Performance levels are associated with recommended proficiency descriptors applicable to each of the relevant competency/skill models listed below.</p> <p><b>Competency/Skill Proficiency Descriptors</b></p> <p>I-Entry: Basic understanding of concepts addressed in relevant competency/skill models</p> <p>II-Intermediate: Working knowledge and application of relevant competency/skill models in work activities</p> <p>III-Advanced: Advanced application and mastery of relevant competency/skill models</p> <p><b>Relevant Competency/Skills Sources:</b></p> <ul style="list-style-type: none"> <li>OPM GS-2200 Job Family Standard Competencies</li> <li>Clinger-Cohen Core Competencies with an emphasis on <i>Technical, Desktop Technology Tools, and IT Security/Information Assurance</i> competency areas (<a href="http://www.cio.gov">www.cio.gov</a>)</li> <li>DHS EBK Competencies</li> <li>FISMA Guidance</li> <li>OPM's IT Workforce Roadmap</li> <li>NIST SP 800-16, Revision 1</li> <li>ODNI Cyber Subdirectory Competencies</li> <li>DoD Directive 8570</li> <li>CNSS Policies, Directives, and Reports</li> </ul>	<ul style="list-style-type: none"> <li>0-3 years experience involving work directly related to systems operations and maintenance (e.g., help desk); OR a Bachelors Degree (suggested areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management)</li> <li>Participation in Scholarship for Service program through a designated Center of Academic Excellence in Information Assurance Education (CAEIAE)</li> </ul>	<ol style="list-style-type: none"> <li>Development Resources:             <ul style="list-style-type: none"> <li>IT Workforce Roadmap (IT Roadmap)</li> <li>Graduate Programs, USDA IT Programs</li> <li>GoLearn Courses (<a href="http://www.golearn.gov">www.golearn.gov</a>)</li> <li>CIO Council (<a href="http://www.cio.gov">www.cio.gov</a>)</li> <li>DoD DISA Training</li> <li>GSA's CIO university Program</li> </ul> </li> <li>University Information Security Programs:             <ul style="list-style-type: none"> <li>National Defense University- IRM College</li> <li>ISIA Degree Programs- CAEIAE</li> <li>Private University Programs (e.g., GMU, MIT)</li> </ul> </li> <li>OPM Development Center: The Federal Executive Institute and the Management Development Centers</li> <li>Participation in coaching/mentoring/job shadowing programs</li> <li>Agency Requirements: organization and business area training identified as required</li> <li>Clinger-Cohen Core Competency-based training sources and Capital Planning and Investment Control (CPIC) mandate</li> <li>Current and emerging legislation, policy, and regulations (e.g., FISMA, NIST SP-800 series, FIPS, OMB directives, CNSSI No. 4012)</li> <li>Training by external vendors for security configuration (e.g., Oracle, Computer Associate, IBM, and HP Tools, Sans Institute)</li> </ol>
<b>II: Intermediate</b>	<p>Applies an understanding of the information security operational characteristics of a variety of computer platforms, networks, software applications, and operating systems</p> <p>Ability to explain to others the methods and techniques used in installation, testing, network debugging, troubleshooting, and maintenance of PCs, servers, printers, and related equipment</p> <p>Automates repetitive processes (e.g., log reviews, configuration testing) to facilitate information security operations</p> <p>Evaluates and assesses operating practices to determine adequate risk management and compliance standards, with on-going systems monitoring</p> <p>Is responsible for contributing, with limited supervision, to projects, programs, and initiatives with medium-threat and moderate scope (e.g., sub-organization wide)</p>		<ul style="list-style-type: none"> <li>Bachelors Degree and 2+ years experience (suggested areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); OR 3-5 years experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs</li> <li>Possession and demonstrated application of relevant certifications             <ul style="list-style-type: none"> <li>Core: MCSE, CCNA, CCNP, ISC<sup>2</sup> CAP</li> <li>Related: CISSP, CISM, ISC<sup>2</sup> ISSMP, CompTIA, SANS GIAC, PMP</li> </ul> </li> </ul>	
<b>III: Advanced</b>	<p>Effectively communicates technical information to non-technical audiences; influences others to comply with policies and conform to standards and best practices</p> <p>Designs the organization's working information security systems operations and maintenance strategy and methodology to comply with the organization's standards and mission</p> <p>Understands the needs of the organization and establishes appropriate vendor relationships to manage the proposal and purchasing process</p> <p>Attends and participates in professional conferences to stay abreast of new trends and innovations in the field of information systems</p> <p>Independently manages, plans, evaluates, and advocates for information security compliance systems, plans, and functions, and is responsible for the management of complex projects, programs, and initiatives with high threat and large scope (e.g., agency-wide or inter-governmental), with on-going systems monitoring</p>		<ul style="list-style-type: none"> <li>Bachelors Degree and 3+ years experience (preferred areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); OR 5+ years of experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs</li> <li>Demonstrated experience in managing/supervising a systems operations and maintenance group</li> <li>Possession and demonstrated application of relevant certifications             <ul style="list-style-type: none"> <li>Core: MCSE, CCNA, CCNP, ISC<sup>2</sup> CAP</li> <li>Related: CISSP, CISM, ISC<sup>2</sup> ISSMP, CompTIA, SANS GIAC, PMP</li> </ul> </li> </ul>	



# Chief Information Security Officer : US Govt – Job Spec

## INFORMATION SECURITY WORKFORCE DEVELOPMENT MATRIX\*

**CHIEF INFORMATION SECURITY OFFICER\*\*:** The Chief Information Security Officer (CISO) is responsible for the information security strategy within an organization. The CISO establishes, implements, and monitors the development and subsequent enforcement of the organization's information security program (i.e., policies, procedures, security architecture standards, security awareness and training program, IT contingency plans, IT security compliance issues). The CISO leads the evaluation and assessment of the security program to ensure that all aspects are in compliance with security requirements, while understanding security threats and vulnerabilities to operations and the organization's environment. The CISO is responsible for information security risk management (e.g., determines risk impact, establishes risk mitigation plans and programs, works with business owners to devise processes for risk assessment) within the organization. The CISO manages the incidents response program (e.g., identifies, reports, and remediates incidents).

Performance Level	Description/Complexity	Competencies/Skills	Suggested Credential	Suggested Learning & Development Sources
III: Advanced	<p>Demonstrates an in depth understanding of enterprise-wide, multi-platform operating systems security, network security, application security, database security, regulatory compliance, incident and risk management</p> <p>Identifies, understands, manages, and interprets information security risks and threats as it affects the business and aligns the information security strategy to achieve organizational mission</p> <p>Designs the organization's information security governance framework to facilitate the implementation of the organization's information security strategy</p> <p>Set expectations, determines appropriate security measures to be used across the department/agency, and maintains governance over the standards and methodologies for information security risk management and compliance reviews</p> <p>Independently manages, plans, evaluates, and advocates for information security solutions, plans, and functions, and is responsible for the management of complex projects, program, and initiatives with high threat and large scope (e.g., organization-wide or inter-governmental)</p> <p>Leads, enables, and is accountable for the implementation and integration of solutions to ensure information security within the organization</p> <p>Understands mechanisms for securing new technologies; understands the impact of new and emerging technologies on the information security environment, as well as tools and methods for mitigating risks</p>	<p>Performance levels are associated with recommended proficiency descriptors applicable to each of the relevant competency/skill models listed below</p> <p><b>Competency/Skill Proficiency Descriptors</b></p> <p>III-Advanced: Advanced application and mastery of relevant competency/skill models</p> <p><b>Relevant Competency/Skill Sources:</b></p> <ul style="list-style-type: none"> <li>▶ NIST SP 800-100 Information Security Handbook: A Guide for Managers</li> <li>▶ OPM GS-2200 Job Family Standard Competencies</li> <li>▶ Clinger-Cohen Core Competencies with an emphasis on <i>Technical, Desktop Technology Tools</i>, and <i>IT Security/Information Assurance</i> competency areas</li> <li>▶ DHS EBK Competencies</li> <li>▶ FISMA Guidance</li> <li>▶ OPM's IT Workforce Roadmap</li> <li>▶ NIST SP 800-16, Revision 1</li> <li>▶ ODNI Cyber Subdirectory Competencies</li> <li>▶ DoD Directive 8570</li> <li>▶ CNSS Policies, Directives, and Reports</li> <li>▶ OPM's Executive Core Qualifications (ECQs) (for SES positions)</li> <li>▶ Additional Key Competencies identified for this role (for senior management positions): <ul style="list-style-type: none"> <li>• Leadership &amp; People Management</li> <li>• Written &amp; Oral Communication</li> <li>• Creative Problem Solving</li> <li>• Budget Formation &amp; Allocation</li> <li>• Project/Program Management</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>▶ Graduate Degree with 5+ years experience (suggested areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); OR 8+ years of experience involving work with transferable skills related to information security, incident and risk management</li> <li>▶ Demonstrated experience in leading an Information Security/IA compliance group</li> <li>▶ Possession and demonstrated application of relevant certifications <ul style="list-style-type: none"> <li>▶ Core: CISSP, CISM, CISA, GSLC</li> <li>▶ Related: ISSMP, CIW-Security, CAP, COMPTIA</li> </ul> </li> <li>▶ Security clearance commensurate with organizational requirements</li> </ul>	<ol style="list-style-type: none"> <li>University Information Security Programs: <ul style="list-style-type: none"> <li>▶ National Defense University- IRM College</li> <li>▶ IS/IA Degree Programs- CAEIAE</li> <li>▶ Private University Programs (e.g., GMU, MIT)</li> </ul> </li> <li>OPM Development Center; The Federal Executive Institute and the Management Development Centers</li> <li>Attendance at industry conferences, work groups, and briefings (i.e., DHS- GFirst; FIA; Black Hat; RSA; ISACA; SANS FIRE; CAISSWG; AFCEA)</li> <li>Development Resources: <ul style="list-style-type: none"> <li>▶ IT Workforce Roadmap (IT Roadmap)</li> <li>▶ Graduate Programs, USDA IT Programs</li> <li>▶ GoLearn Courses (<a href="http://www.golearn.gov">www.golearn.gov</a>)</li> <li>▶ CIO Council (<a href="http://www.cio.gov">www.cio.gov</a>)</li> <li>▶ DoD DISA Training</li> <li>▶ AFCEA (<a href="http://www.afcea.org">www.afcea.org</a>)</li> <li>▶ CAISSWG</li> <li>▶ GSA's CIO University Program</li> </ul> </li> <li>Participation in coaching/mentoring/job shadowing programs</li> <li>Agency Requirements: organization and business area training identified as required</li> <li>Current and emerging legislation, policy, and regulations (e.g., FISMA, NIST SP-800 series, FIPS, OMB directives, CNSSI No. 4011 &amp; 4012)</li> <li>Training by external vendors (e.g., Sans Institute, ISC², ISACA, MIS)</li> </ol>

# **\* Workshop Session 10 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Cybersecurity Capacity Building and International Collaboration & Resources***

<b>1 – Aim: Cyber Skills Building</b>	<b>2 – National Cyber Framework</b>	<b>3 – Cybersecurity Skill Needs</b>
<b>4 – Cyber Skills Certification</b>	<b>5 – Training &amp; Awareness</b>	<b>6 – Public-Private Partnerships</b>
<b>7 – International Collaboration</b>	<b>8 – Next Steps for Jamaica</b>	<b>9 – On-Line Cyber Resources</b>





# National Cyber Skills Framework

- Jamaica needs to build cybersecurity skills capacity within the context of its national cybersecurity framework, led by the proposed NCA
- The skills development programme will be an on-going multi-year programme and should be undertaken by the government in partnership with key security stakeholders including:
  - Academic & Research Institutions such as the University of Technology
  - Awareness Programmes with High Schools through games & competitions such as the UK and US Government “Cyber Challenge” Programmes
  - ICT Market Sector, including the major Telecomms, ISP & Mobile Players
  - Critical Service Sector Businesses including Energy, Financial & Travel
- The Government should provide some financial support to “kick-start” the programme which should initially run for 3 to 5 years, with the objective to train-up professionally certified cybersecurity specialists



# **\* Workshop Session 10 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Cybersecurity Capacity Building and International Collaboration & Resources***

<b>1 – Aim: Cyber Skills Building</b>	<b>2 – National Cyber Framework</b>	<b>3 – Cybersecurity Skill Needs</b>
<b>4 – Cyber Skills Certification</b>	<b>5 – Training &amp; Awareness</b>	<b>6 – Public-Private Partnerships</b>
<b>7 – International Collaboration</b>	<b>8 – Next Steps for Jamaica</b>	<b>9 – On-Line Cyber Resources</b>

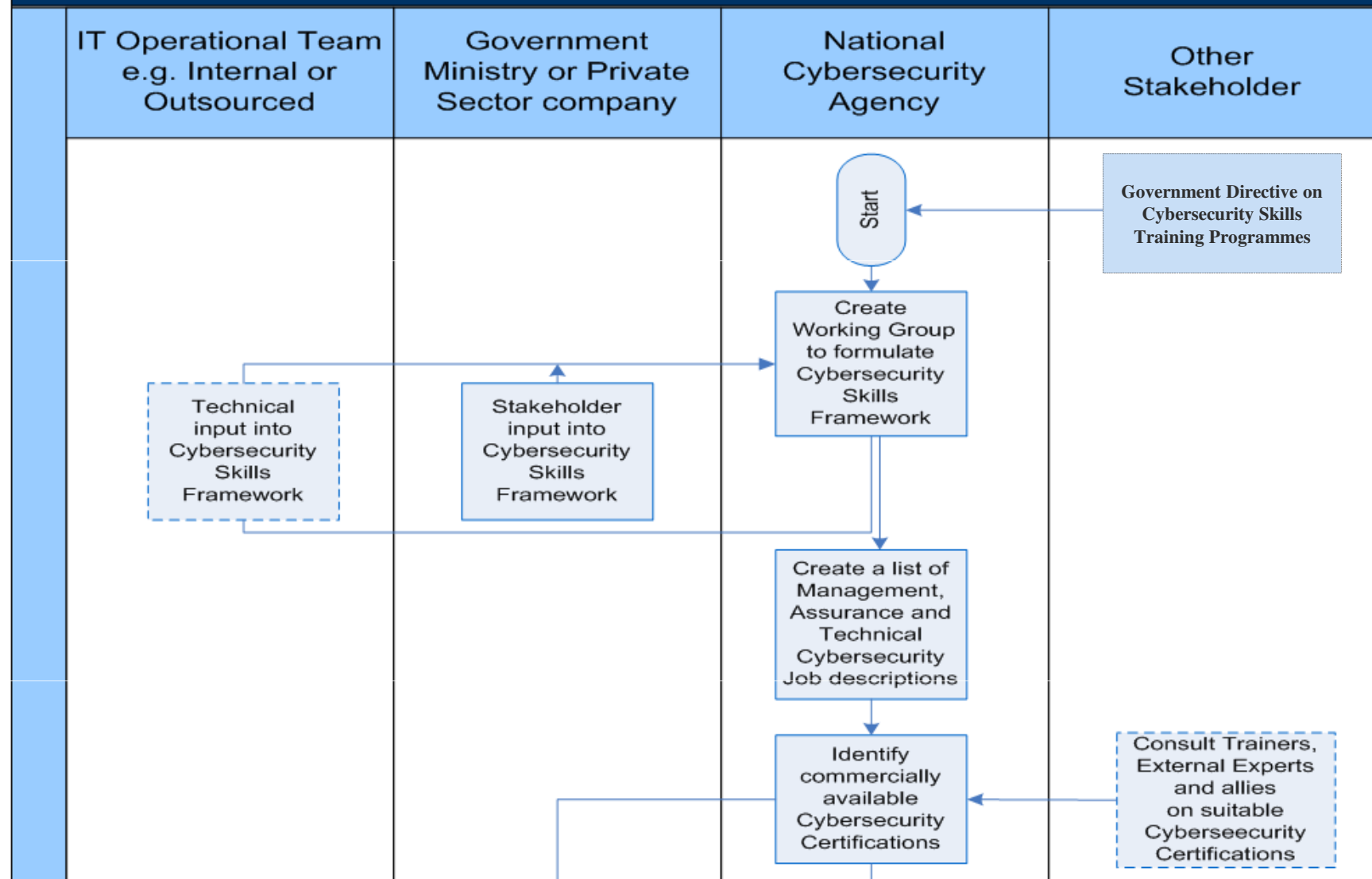


# Cybersecurity Skills Needs

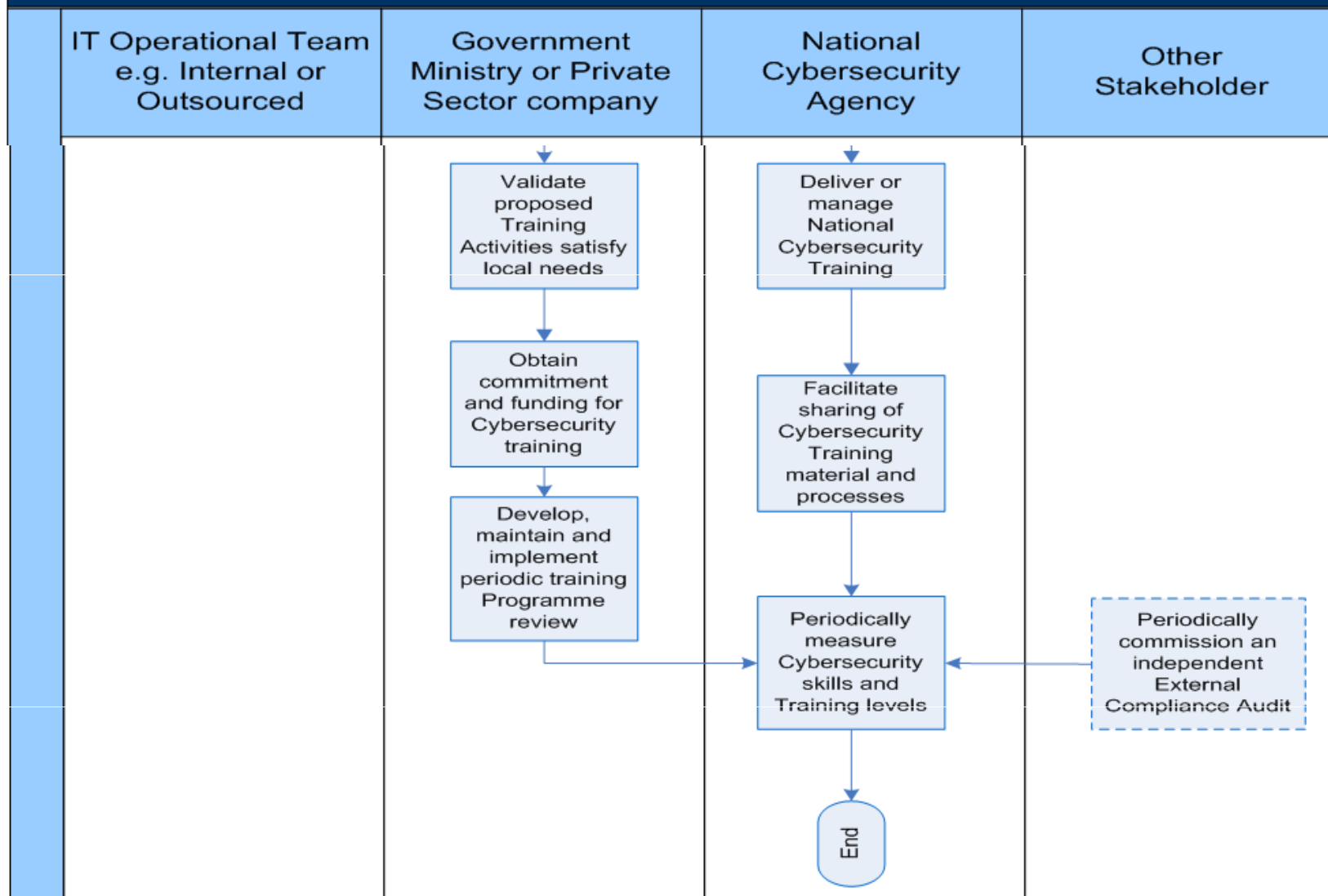
Management	Information Assurance	Technical
<ul style="list-style-type: none"> <li>• Cybersecurity business case formulation</li> <li>• IT Base skills</li> <li>• Staff Management skills/ Leadership skills</li> <li>• Personnel Security</li> <li>• Multi-Disciplinary skills (technology, people etc)</li> <li>• Communication skills</li> <li>• Cyber-Criminal Psychology</li> <li>• Cyber-Ethics Skills</li> <li>• Data ownership</li> </ul>	<ul style="list-style-type: none"> <li>• Cybersecurity Policies, Standards and Procedures</li> <li>• Risk Management</li> <li>• System Accreditation</li> <li>• Compliance Checking</li> <li>• Audit and Monitoring</li> <li>• User Rights and Responsibilities</li> <li>• Incident Management Process Design</li> <li>• Assurance, trust and confidence mechanisms</li> </ul>	<ul style="list-style-type: none"> <li>• IT technical skills (security management)</li> <li>• IT technical skills (IT defences deployment)</li> <li>• Security Design Principles e.g. zoning</li> <li>• Resilient Infrastructure</li> <li>• Data Protection/ System administration</li> <li>• Cryptographic and Applied Crypto Skills</li> <li>• Data custodianship</li> <li>• Operational Security</li> <li>• Incident Management</li> </ul>



# CYBERSECURITY SKILLS AND TRAINING FRAMEWORK



# CYBERSECURITY SKILLS AND TRAINING FRAMEWORK

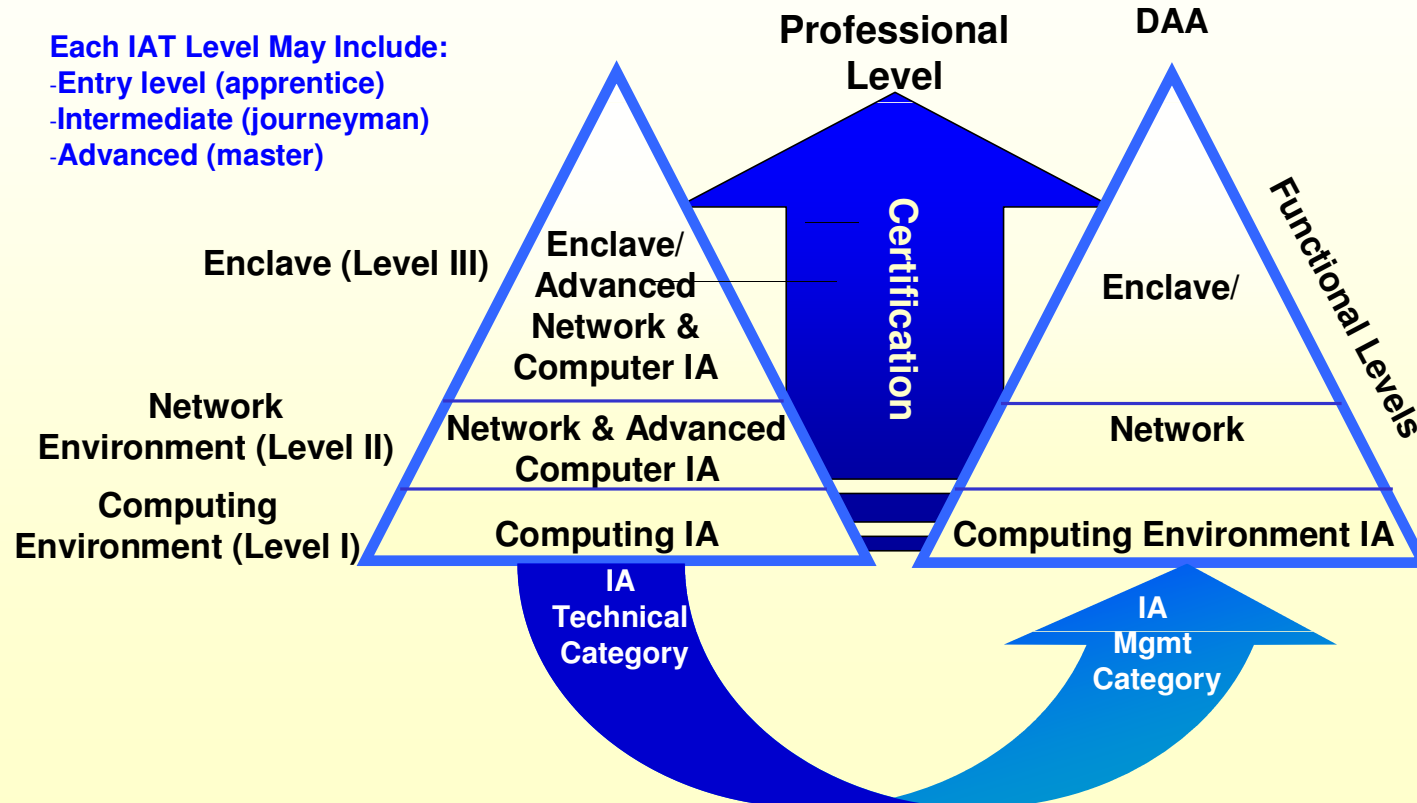




# IA Workforce Structure

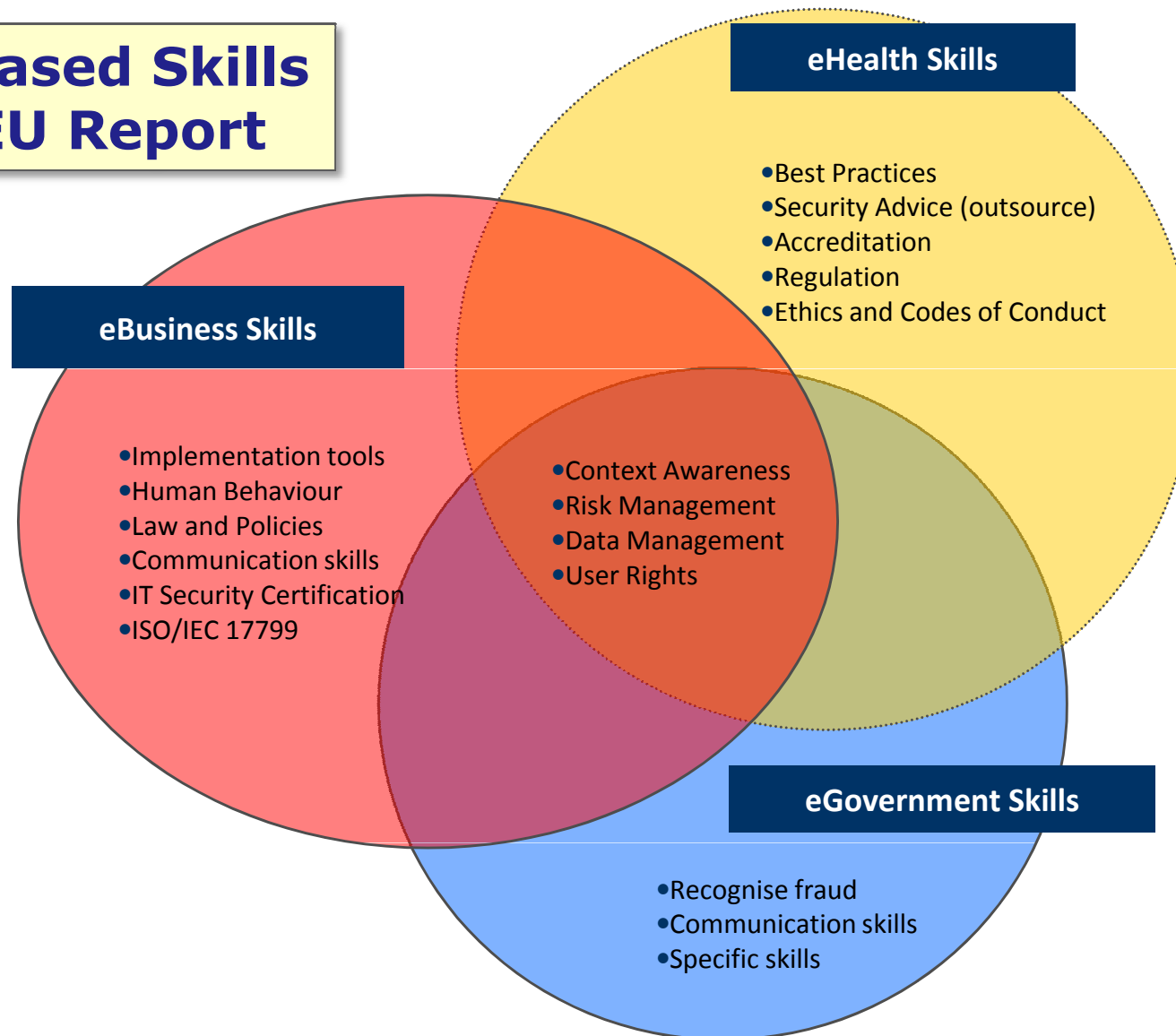


## IA WF Structure





# Sector based Skills From EU Report



# **\* Workshop Session 10 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Cybersecurity Capacity Building and International Collaboration & Resources***

<b>1 – Aim: Cyber Skills Building</b>	<b>2 – National Cyber Framework</b>	<b>3 – Cybersecurity Skill Needs</b>
<b>4 – Cyber Skills Certification</b>	<b>5 – Training &amp; Awareness</b>	<b>6 – Public-Private Partnerships</b>
<b>7 – International Collaboration</b>	<b>8 – Next Steps for Jamaica</b>	<b>9 – On-Line Cyber Resources</b>



# Cyber Skills Certification

- There are many national & international organisations that provide some level of security training, qualification and certifications.
- Within these slides we consider just a few, and focus on the CISSP.
- Certification is not just a “one-off” exercise, since cybersecurity professionals, just like medical doctors, will need to renew and update their qualifications, such as the CISSP every 3 years.
- Jamaican Academic & Training Institutions might consider ways in which they can align their security courses so that students can graduate with an internationally recognised qualification & certification



# CISSP Certification Domains

- The CISSP – Certified Information Systems Security Professional is one of the highest international qualifications from the (ISC)<sup>2</sup>, and is based upon the core tenets of *Confidentiality, Integrity & Availability*:
  - 1) Access Control
  - 2) Application Security
  - 3) Business Continuity and Disaster Recovery
  - 4) Cryptography
  - 5) Information Security and Risk Management
  - 6) Legal, Regulations, Compliance and Investigations
  - 7) Operations Security
  - 8) Physical (Environmental) Security
  - 9) Security Architecture and Design
  - 10) Telecommunications and Network Security
- *An in-depth study of all these security domains would easily fill an intensive 3 month training schedule, but during the 2-day technical workshop on 16<sup>th</sup>/17<sup>th</sup> Sept we'll consider all these topics in some way*



CERTIFICATION PROVIDER	CERTIFICATION NAME
Carnegie Mellon Software Engineering Institute CERT®	Computer Security Incident Handler (CSIH)
Computing Technology Industry Association (CompTIA)	A+
CompTIA	Security+
CompTIA	Network+
International Information Systems Security Certifications Consortium (ISC) <sup>2</sup>	Certified Information Systems Security Professional (CISSP) (or Associate - this means the individual has qualified for the certification except for the number of years experience)
(ISC) <sup>2</sup>	Information Systems Security Architecture Professional (ISSAP)
(ISC) <sup>2</sup>	Information Systems Security Engineering Professional (ISSEP)
(ISC) <sup>2</sup>	Information Systems Security Management Professional (ISSMP)
(ISC) <sup>2</sup>	System Security Certified Practitioner (SSCP)
Information Systems Audit and Control Association (ISACA)	Certified Information Security Manager (CISM)
ISACA	Certified Information Security Auditor (CISA)
Microsoft Corporation	Microsoft Certified System Administrator: Security (MCSA Security)
Security Certified Program	Security Certified Network Professional (SCNP)
Security Certified Program	Security Certified Network Architect (SCNA)
Global Information Assurance Certification (GIAC)	GIAC Certified Intrusion Analyst (GCIA)
GIAC	GIAC Certified Incident Handler (GCIH)
GIAC	GIAC Security Expert (GSE)
GIAC	GIAC Security Essentials Certification (GSEC)
GIAC	GIAC Security Leadership Certificate (GSLC)
GIAC	GIAC Systems and Network Auditor (GSNA)
GIAC	GIAC Information Security Fundamentals (GISF)

# **\* Workshop Session 10 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Cybersecurity Capacity Building and International Collaboration & Resources***

<b>1 – Aim: Cyber Skills Building</b>	<b>2 – National Cyber Framework</b>	<b>3 – Cybersecurity Skill Needs</b>
<b>4 – Cyber Skills Certification</b>	<b>5 – Training &amp; Awareness</b>	<b>6 – Public-Private Partnerships</b>
<b>7 – International Collaboration</b>	<b>8 – Next Steps for Jamaica</b>	<b>9 – On-Line Cyber Resources</b>



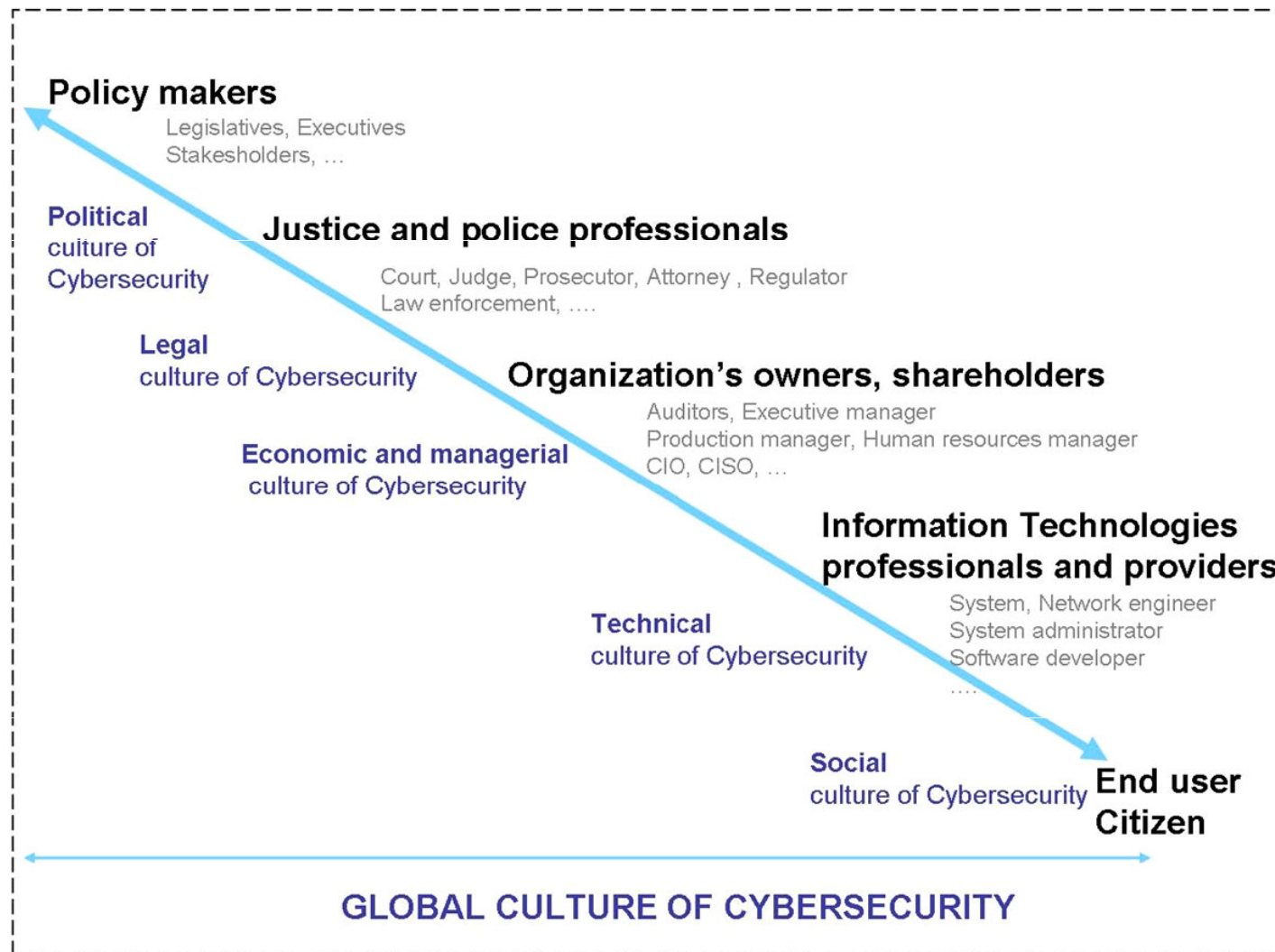


# Cybersecurity Training and Awareness

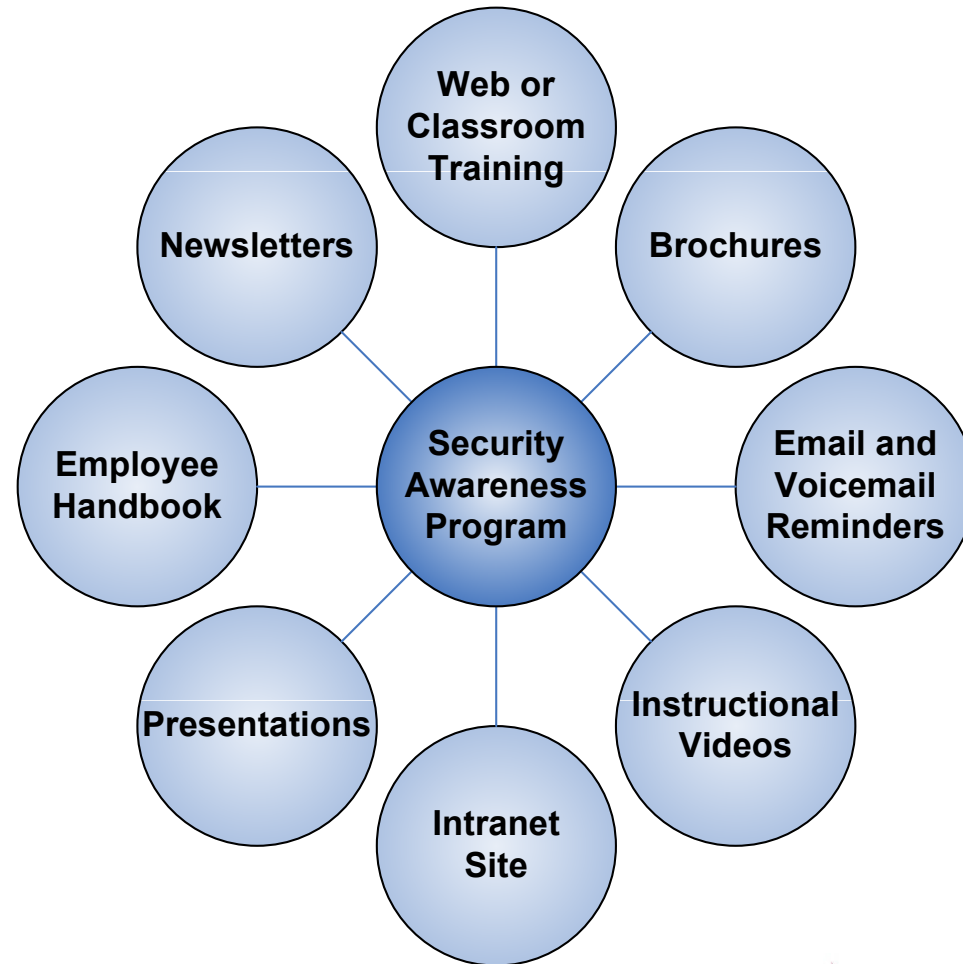
- Cybersecurity training and awareness will need to be tackled as a *multi-sector* and multi-stakeholder programme.
- Ultimately *every* business and *every* citizen will need to become cyber aware if they are to remain safe in the virtual world of cyberspace.
- Public awareness programmes will need strong central government support in order that all citizen segments from children to the elderly become conversant with *cyber risks* & how to protect oneself on-line.
- Awareness Campaigns may target the client sectors through:
  - Brochures, Newsletters and Video Materials
  - Local Discussions Groups held in Schools
  - Employee Handbooks for Staff Awareness
  - Short Training & Awareness Courses
  - Interactive Cybersecurity Website
  - Viral Marketing Campaign through Social Media Sites
- Every media awareness channel is important if Jamaica is to promote & achieve a cybersecurity culture during the coming 3 to 5 years!...



# ITU: Promoting a Culture of Cybersecurity



# Cybersecurity Awareness & Education Techniques



# **\* Workshop Session 10 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Cybersecurity Capacity Building and International Collaboration & Resources***

<b>1 – Aim: Cyber Skills Building</b>	<b>2 – National Cyber Framework</b>	<b>3 – Cybersecurity Skill Needs</b>
<b>4 – Cyber Skills Certification</b>	<b>5 – Training &amp; Awareness</b>	<b>6 – Public-Private Partnerships</b>
<b>7 – International Collaboration</b>	<b>8 – Next Steps for Jamaica</b>	<b>9 – On-Line Cyber Resources</b>



# Public – Private Partnerships (PPP) : Development of CyberSecurity Skills

- The extensive scope required for cybersecurity capacity & skills building mean that a recommended way forward is for the government to negotiate partnerships with the private business sector
- The PPP Model is used extensively in many countries in which the government outsources ICT-based eGov services and training to private sector companies that already have the requisite skills:
  - CERT/CSIRTs may be outsourced to Telecomms/ISPs as well as the University Networks
  - Government ICT Infrastructure, and eGov Applications Hosting can also be outsourced
  - Awareness and Professional Training can be managed through Colleges & Universities
  - Critical Service Sector Skills Building for Cybersecurity will be developed in partnership with the relevant sector such as banking/finance, energy, agriculture, travel and tourism
- Using PPP will significantly accelerate the rate at which the Jamaican Government can implement its cybersecurity action plan & roadmap whilst at the same time sharing the investment cost with business.



# **\* Workshop Session 10 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Cybersecurity Capacity Building and International Collaboration & Resources***

<b>1 – Aim: Cyber Skills Building</b>	<b>2 – National Cyber Framework</b>	<b>3 – Cybersecurity Skill Needs</b>
<b>4 – Cyber Skills Certification</b>	<b>5 – Training &amp; Awareness</b>	<b>6 – Public-Private Partnerships</b>
<b>7 – International Collaboration</b>	<b>8 – Next Steps for Jamaica</b>	<b>9 – On-Line Cyber Resources</b>



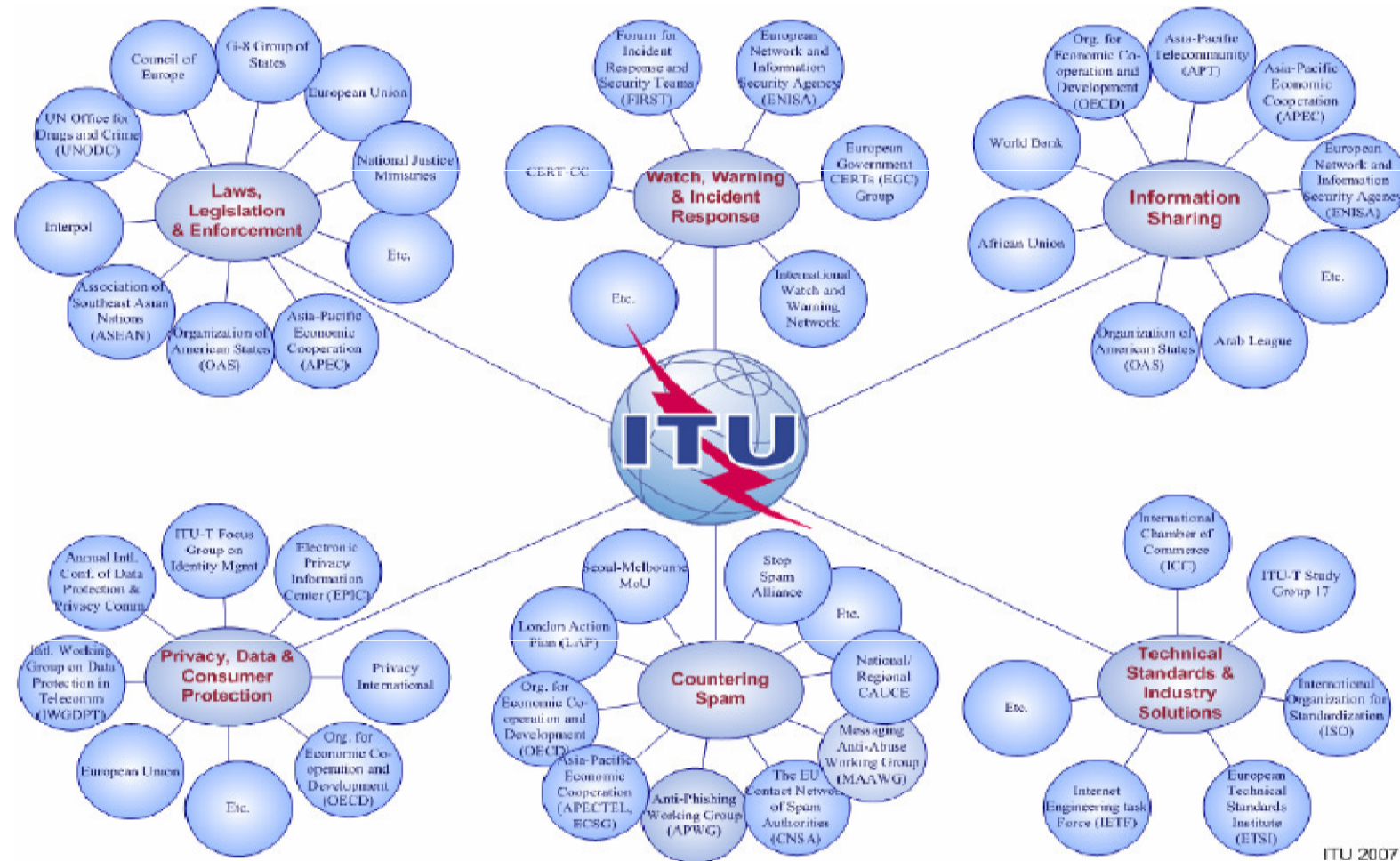


# International Collaboration

- Cybersecurity is a global trans-border issue. Cybercrime can only be managed through strong international collaboration and partnerships
- The ITU Global Cybersecurity Agenda tackles this through multiple partnerships including its role within the IMPACT Alliance, and its NEWS and ESCAPE Programmes, as well as in-depth skills training
- INTERPOL is also a critically important partner for Jamaica in the investigation of international cybercrime “rings” & cyberterrorist “cells”
- CERTs/CSIRTS also have well connected international communities that enable member countries to support each other during cyber attacks



# International Stakeholders for the Cybersecurity Ecosystem



ITU 2007



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



International  
Telecommunication  
Union

Committed to connecting the world

# National CSIRT Network: Europe & Asia



More than 50 Countries are members of the worldwide network of CSIRTs  
(Interactive Map from [www.cert.org](http://www.cert.org) )



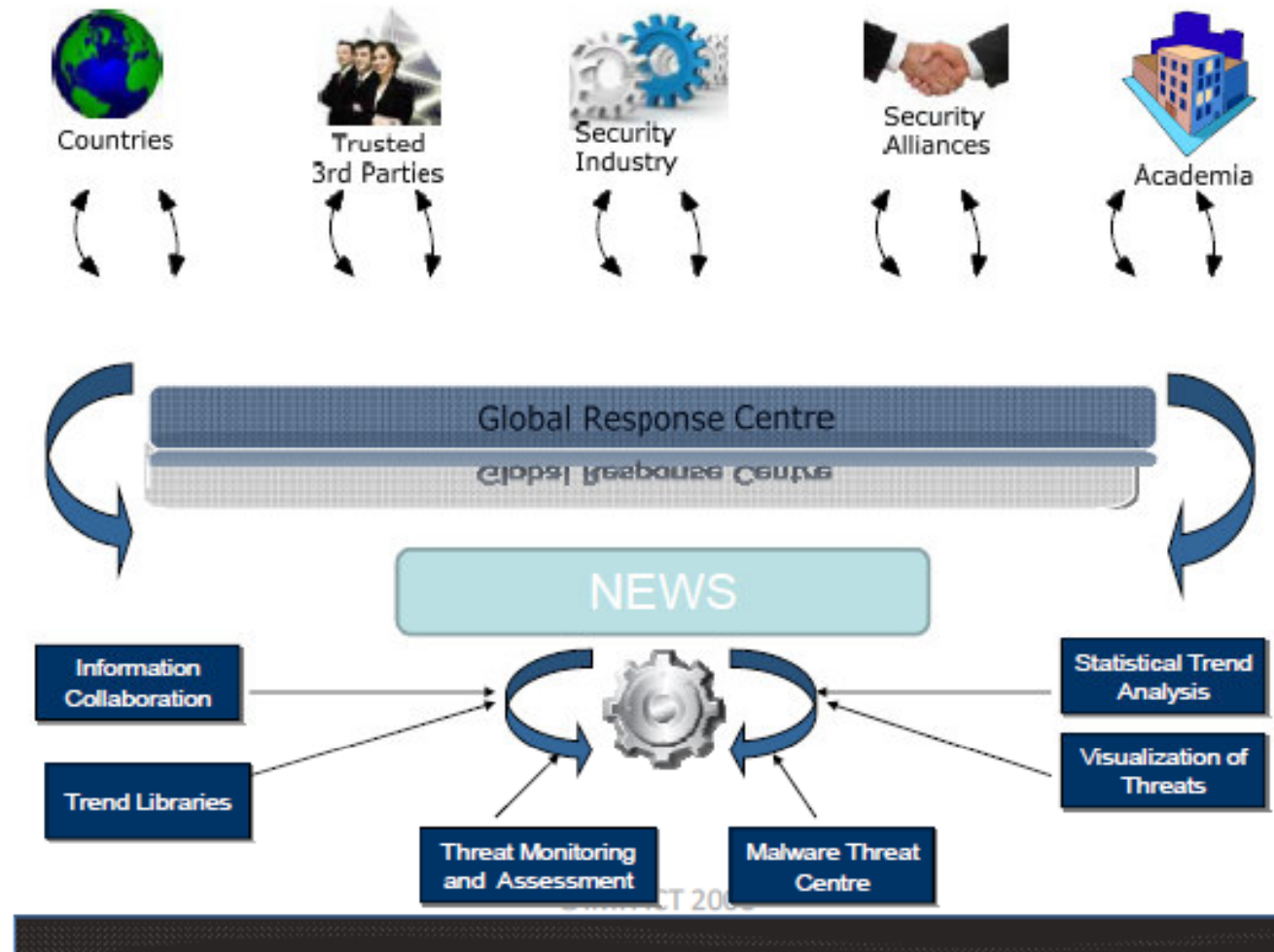
University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world

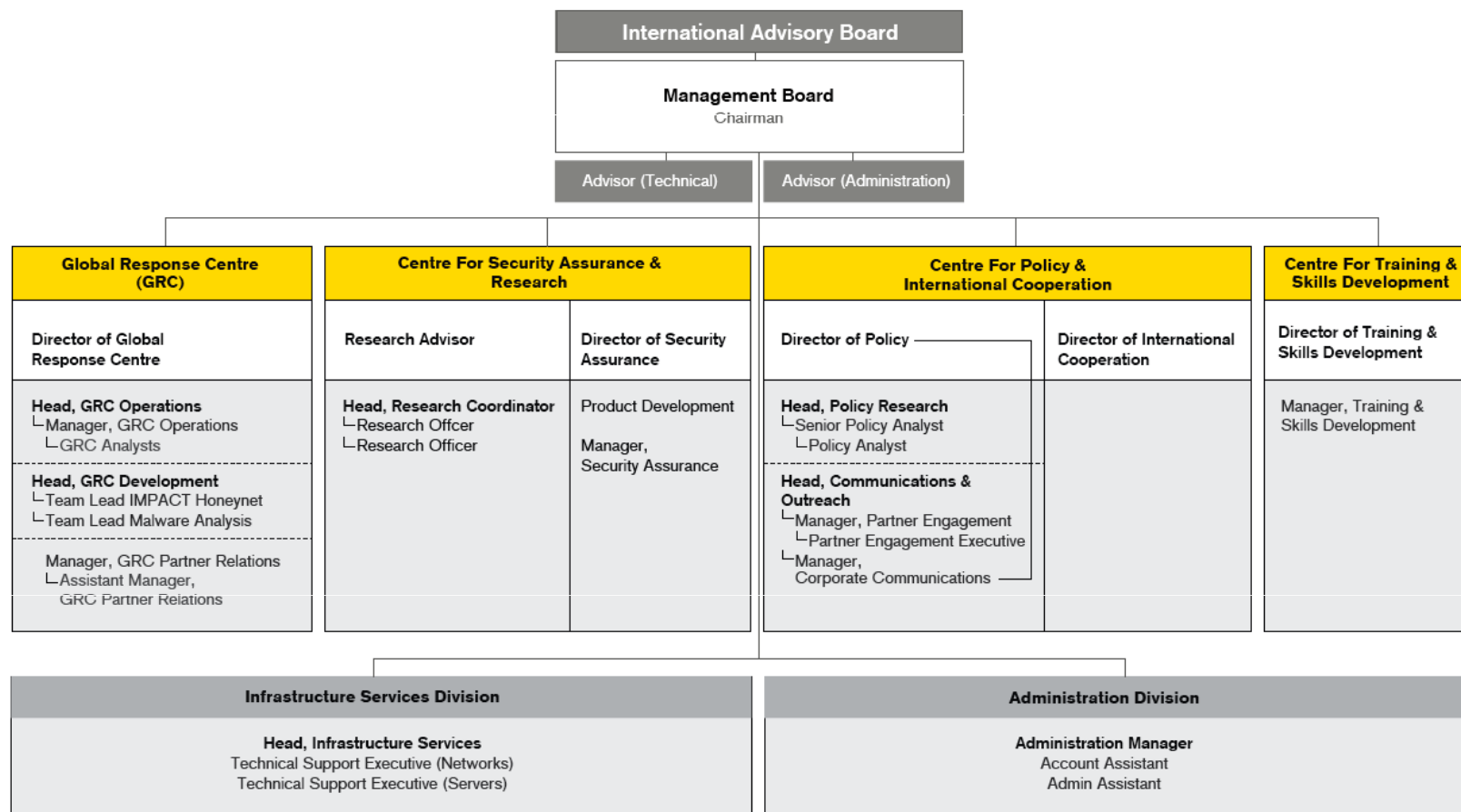
# Network Early Warning System(NEWS)



# Worldwide IMPACT Alliance

**IMPACT**

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world



# IMPACT Global Headquarters: Cyberjaya, Malaysia

## IMPACT Global Headquarters

IMPACT's Global HQ was launched on 20<sup>th</sup> May 2009 by the 5<sup>th</sup> Prime Minister of Malaysia, The Honourable Dato' Seri Abdullah Ahmad Badawi, witnessed by the current Prime Minister of Malaysia, The Honourable Dato' Sri Najib Tun Razak and the Secretary-General of the ITU, Dr. Hamadoun Touré.

The IMPACT's Global HQ is located on a seven acre estate near Kuala Lumpur with a current infrastructure of over 58,000 square feet. Its extensive infrastructure includes the Global Response Centre (GRC) – a state of the art centre for cyber threats detection, analysis and response – alongside well-equipped training rooms, research labs, an auditorium, meeting facilities and administrative offices. IMPACT is staffed by a global workforce.

IMPACT's Global HQ is also the physical and operational home of the Global Cybersecurity Agenda (GCA), a framework for international cooperation initiated by the International Telecommunication Union (ITU). The GCA is aimed at finding strategic solutions to boost confidence and security in an increasingly networked information society.

Besides the GRC, the facility is purpose built to house IMPACT's four Centres, which were formed around the four key functions of IMPACT.



**IMPACT = International Multilateral Partnerships Against Cyber Threats**



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world



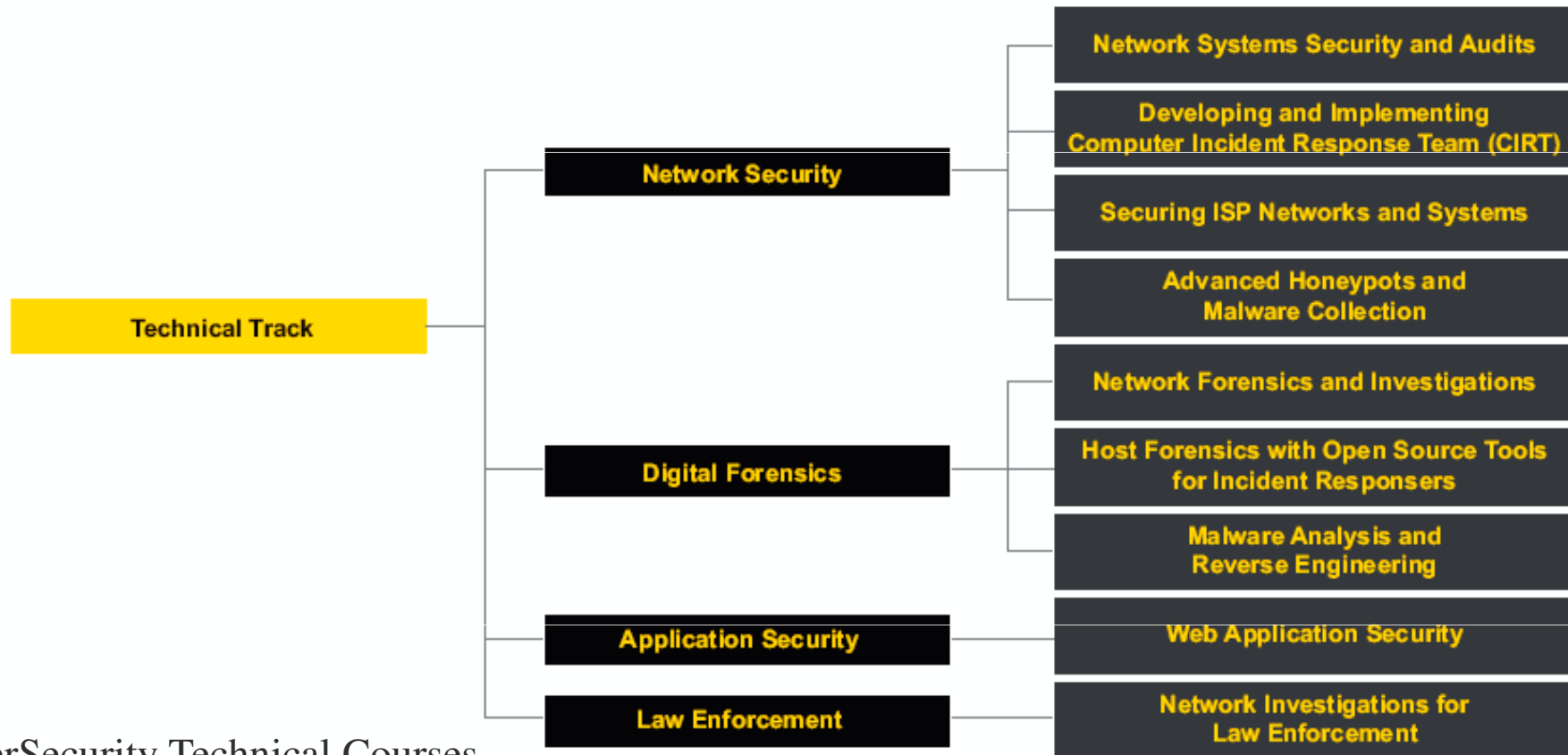
# IMPACT: Cyber Training Roadmap

## IMPACT Training Roadmap

	Management Track			Technical Track			
	Security Management	Security Audit	Legal & Policy Framework	Network Security	Digital Forensics	Application Security	Law Enforcement
Target Audience	CIO, CISO, IT Security Manager, IT Security Executive, Compliance Manager, Dept. Head, Manager, Executive	Internal Auditor, External Auditor, Risk Manager, Compliance Manager, IT Security Manager	Law Students & Practitioners, IT Students & Professionals, Police & Law Enforcement Officers, Management Students & Professionals	Network Administrator/ Support, Incident Handlers, Network Managers, IT Support/ Administrators, CIRT Analyst	Forensics Analyst, Forensics Investigators, Incident Handlers, Malware Analyst	Web Application Developer, Webmasters, Application Support Executive	Police Officers, Law Enforcement Officers, Legal Officers, Lawyers
Foundation	IMPACT SecurityCore - Information Security Fundamentals + Security Awareness for Everyone/ Managers/IT Administrators						
Intermediate	Developing Security Policies & Procedures  ISO 27001 Information Security Management (ISMS) Concepts and Awareness  ISO 27001 Information Security Management (ISMS) Implementation	ISO 27001 Information Security Management System Lead Auditor (ISMS)	Cyber Crime: Domestic and International Models of Cooperation  Legal Responses to Emerging Cyber Crimes	Network Systems Security and Audits  Developing and Implementing Computer Incident Response Team (CIRT)  Securing ISP Networks and Systems  Advanced Honeypots and Malware Collection	Network Forensics and Investigations  Host Forensics with Open Source Tools for Incident Responders  Malware Analysis and Reverse Engineering	Web Application Security	Network Investigations for Law Enforcement
Advanced	(ISC) <sup>2</sup> CISSP CBK Review Seminar	(ISC) <sup>2</sup> CISSP CBK Review Seminar	(ISC) <sup>2</sup> CISSP CBK Review Seminar	(ISC) <sup>2</sup> CISSP CBK Review Seminar	(ISC) <sup>2</sup> CISSP CBK Review Seminar	(ISC) <sup>2</sup> CISSP CBK Review Seminar	(ISC) <sup>2</sup> CISSP CBK Review Seminar



# IMPACT: Cybersecurity Technical Training

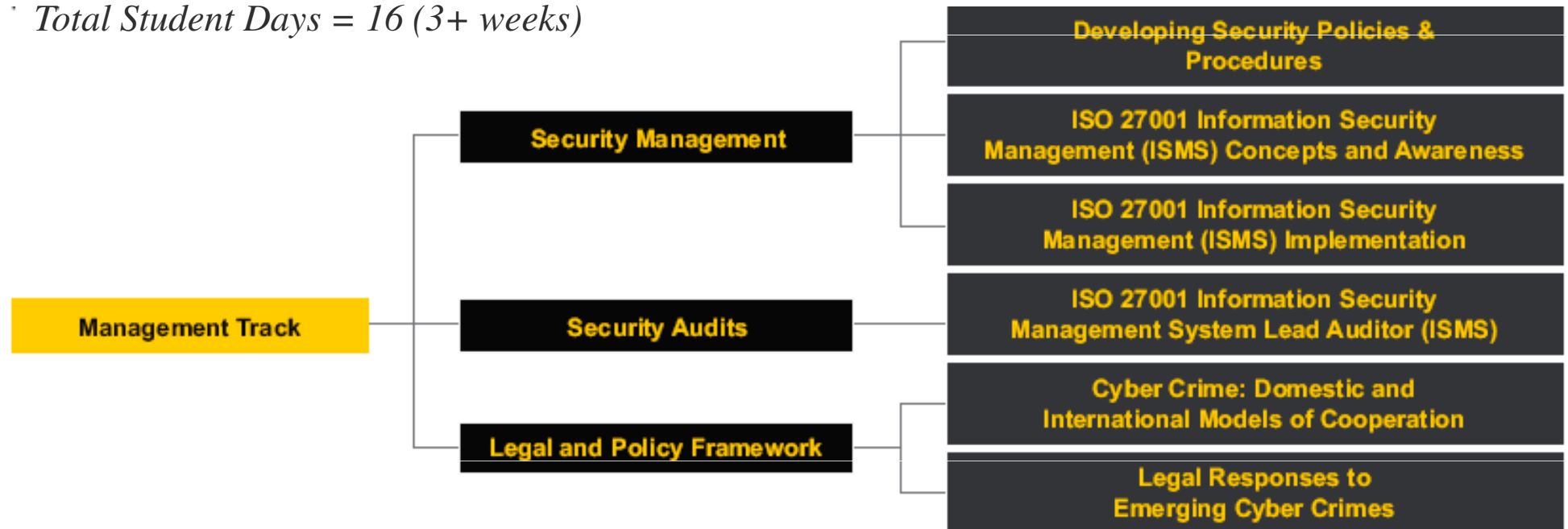


CyberSecurity Technical Courses  
*Total Student Days = 41 (8+ Weeks)*

# IMPACT: Cyber Management Training

CyberSecurity Management Courses

· *Total Student Days = 16 (3+ weeks)*



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



Committed to connecting the world

# IMPACT : Worldwide Alliance

IMPACT International Partners: ITU, UN, INTERPOL and CTO



Industry Partners include: Symantec, Kaspersky Labs, Cisco, Microsoft, (ISC)<sup>2</sup>, F-Secure, EC-Council, Iris, GuardTime, Trend Micro and the SANS Institute



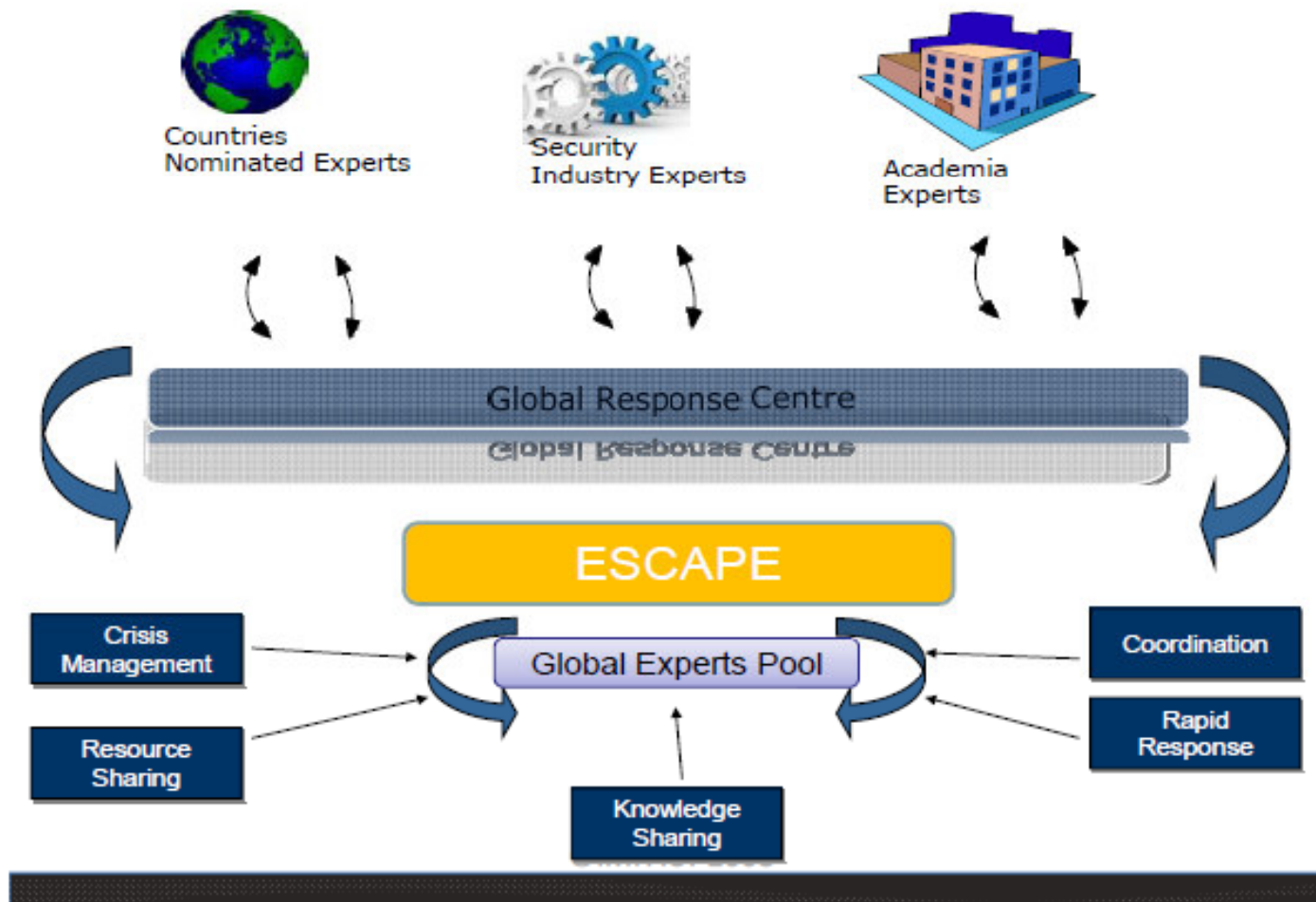
University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica

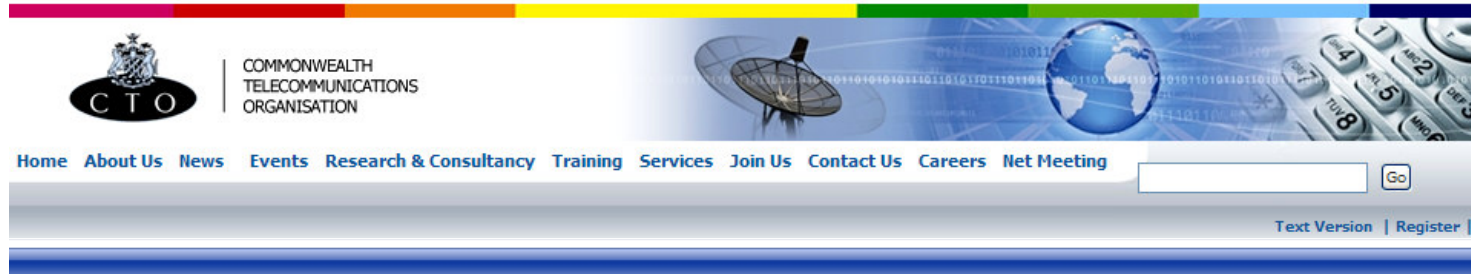


Committed to connecting the world

# Electronically Secure Collaboration Platform for Experts (ESCAPE)



# Commonwealth Telecommunications Organisation – IMPACT Alliance Partner



Home > About CTO Events > About Cybersecurity

## About CTO Events



### Cybersecurity Forum

#### Background

With the critical information infrastructure of Estonia coming under attack in 2007, the focus of Cyber security was elevated from an individual perspective to a National perspective. Importantly this incident highlighted the need for developing countries to implement robust and effective Cybersecurity frameworks, without which the entire Cyber World will be at risk.

The CTO's Cybersecurity Conference aims to:

- Create awareness of the many facets of cyber threats and alert stakeholders of the need to adopt robust Cybersecurity frameworks
- Build capacity of the key decision makers in developing countries to implement strategies aimed at preventing and responding to the growing menace of Cyber threats
- Provide the key decision makers with the means to adopt resilient technical measures, establish appropriate organisational structures and create robust legal/regulatory frameworks
- Promote international cooperation in Cybersecurity to help developing countries to leverage the strengths of developed countries
- Broker partnerships between the different players in Cybersecurity to facilitate the flow of information, expertise and resources



University of Technology,  
Jamaica

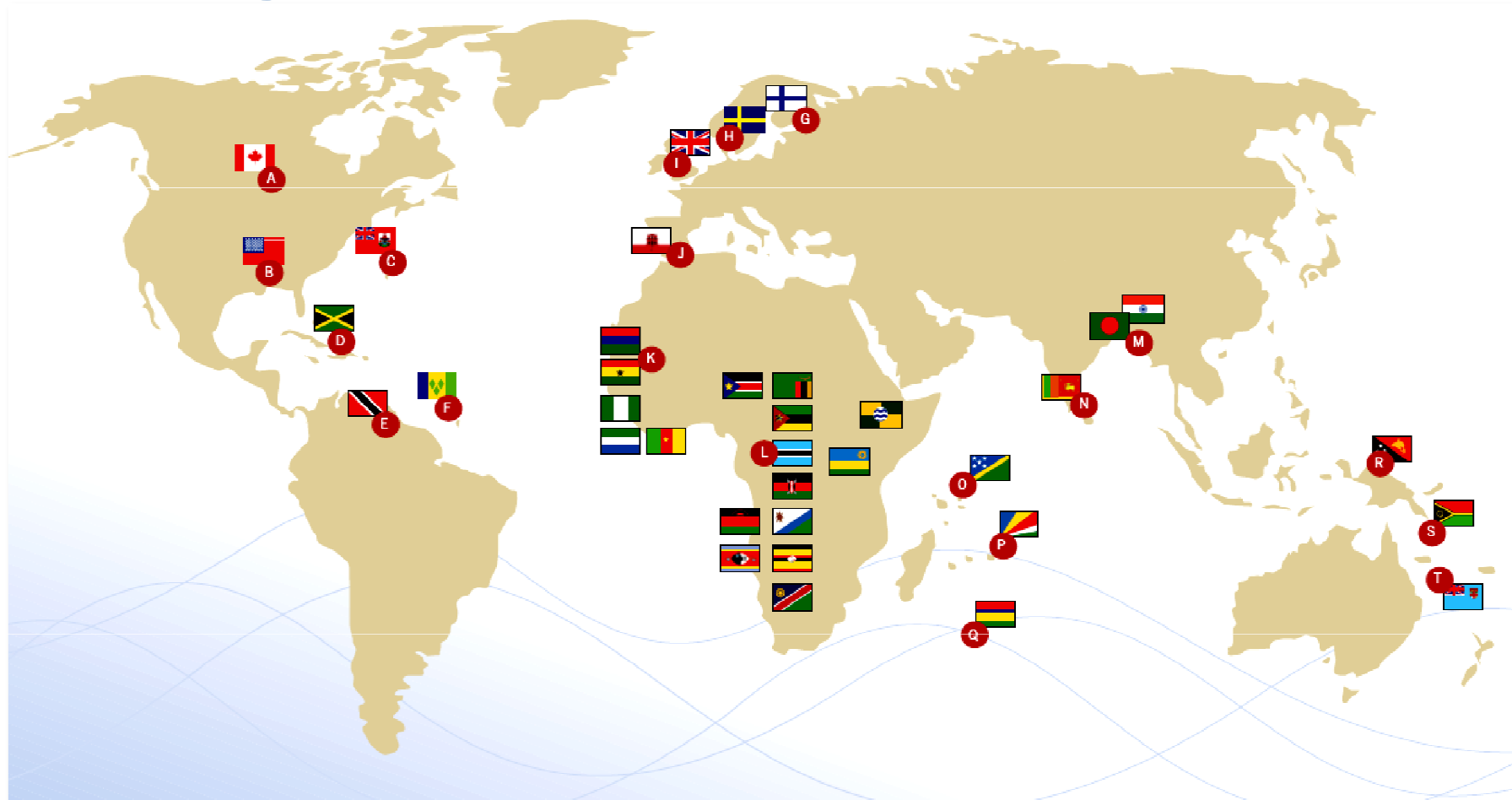
**ITU Centres of Excellence Network for the Caribbean Region**  
**Developing a National and Organizational Cybersecurity Strategy**  
*13-15 September, Kingston, Jamaica*



**Committed to connecting the world**



# Commonwealth Telecomms Organisation ([www.cto.int](http://www.cto.int))



Jamaica: Office of Utilities Regulation – (OUR)



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



International  
Telecommunication  
Union

Committed to connecting the world

# International Collaboration : Jamaica and USA – Telemarketing Fraud

The screenshot shows the official website of the U.S. Department of Homeland Security, specifically the U.S. Immigration and Customs Enforcement (ICE) section. The header features the ICE logo, a Google Custom Search bar, and a link to report suspicious activity. The main navigation bar includes links for Home, About, Programs, Careers, News, and Contact. On the left, a 'Quick Links' sidebar lists various resources like ICE Press, Archive, Fact Sheets, and more. The central 'News Releases' section, dated May 27, 2009, features a headline about the U.S. and Jamaica launching an international task force to combat telemarketing fraud. The text of the release describes the Project JOLT task force, its multi-agency nature, and the goal to combat Jamaican-based telemarketing fraud operations that prey on U.S. citizens. It also includes a quote from JCF Commissioner Hardley Lewin and a paragraph detailing the expertise of ICE and the Department of Homeland Security in transnational criminal investigations.

**U.S. and Jamaica launch international task force to combat telemarketing fraud**

KINGSTON, Jamaica - U.S. and Jamaican officials announced the launch of the Project JOLT (Jamaican Operations Linked to Telemarketing) task force on Wednesday. JOLT is an ICE-led, multi-agency, international task force established to combat Jamaican based telemarketing fraud operations that prey on U.S. citizens and others.

"The Jamaican Constabulary Force will work closely with our international partners in order to minimize and eventually eradicate the lottery scams," said JCF Commissioner Hardley Lewin. "We welcome any assistance and for our part will ensure that a calculated effort is undertaken to deal with the lottery scam."

As the Department of Homeland Security's largest investigative agency with special cross-border immigration and customs authorities and extensive international money laundering investigative expertise, U.S. Immigration and Customs Enforcement (ICE) with its 54 offices in 42 countries, has significant expertise in transnational criminal investigations.

# **\* Workshop Session 10 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Cybersecurity Capacity Building and International Collaboration & Resources***

<b>1 – Aim: Cyber Skills Building</b>	<b>2 – National Cyber Framework</b>	<b>3 – Cybersecurity Skill Needs</b>
<b>4 – Cyber Skills Certification</b>	<b>5 – Training &amp; Awareness</b>	<b>6 – Public-Private Partnerships</b>
<b>7 – International Collaboration</b>	<b>8 – Next Steps for Jamaica</b>	<b>9 – On-Line Cyber Resources</b>



# Next Steps for Jamaica

- During this intensive 3 day workshop we've covered all the 5 pillars of ITU's comprehensive Global Cybersecurity Agenda
- Some key actions for Jamaica during the next 12 months are:
  - Establish a National Cybersecurity Agency (or Council) with PM & Cabinet Level Authority
  - Review the Legislation and Regulations, and ways in which Jamaica can extend the Cyber Crimes Act to further secure the nation in Cyberspace, against Cybercrimes & Terrorism
  - Promote a culture of cybersecurity understanding and awareness across business & citizens
  - Facilitate the organisation of professional training within academic & educational institutions
  - Ensure that the Jamaican Government and Enterprises are supported by a national CERT/CSIRT
  - Extend the professional experience & skills of the OCID Cyber Crime Team in Digital Forensics
  - Implement PPP Agreements to outsource Government Cybersecurity Programmes to Business
  - Promote International Collaboration through regional (Caribbean) and global partnerships

*.....this afternoon we'll work together to develop practical cybersecurity roadmaps for the Government and selected critical service sectors*



# **\* Workshop Session 10 \***

## **ITU Global Cybersecurity Agenda:**

### ***...Cybersecurity Capacity Building and International Collaboration & Resources***

<b>1 – Aim: Cyber Skills Building</b>	<b>2 – National Cyber Framework</b>	<b>3 – Cybersecurity Skill Needs</b>
<b>4 – Cyber Skills Certification</b>	<b>5 – Training &amp; Awareness</b>	<b>6 – Public-Private Partnerships</b>
<b>7 – International Collaboration</b>	<b>8 – Next Steps for Jamaica</b>	<b>9 – On-Line Cyber Resources</b>



# On-Line Cybersecurity Resources

- *ITU Cybersecurity Toolkits*, Reports and Standards
  - ITU Cybercrime Toolkit & Cybercrime Guidelines for Developing Countries
  - ITU Toolkit on “Botnet” Mitigation – *Protection against Denial of Service Attacks*
  - ITU Self-Assessment Toolkit for CIIP – Critical Information Infrastructure Protection
  - ITU Technical Security Standards such as X.800 Series and the X.1200 Series
- *Technical Publications* on Cybersecurity from NIST, ISF, ISO, ENISA well as the Cybersecurity Organisations from national Governments
  - NIST – National Institute of Standards and Technology (“800” Security Series)
  - ENISA – European Network & Information Security Agency
  - ISF – Information Security Forum
  - ISO – International Standards Organisation
- *Industry White Papers* and Reports from the major ICT Cybersecurity Companies such as Symantec, Sophos, Kaspersky Labs and McAfee
- *On-Line “Google” Searches* generate 15Mil+ “hits” from “cybersecurity”, whilst a refined search will provide *daily news* updates & *latest reports*





# ITU: On-Line Video Channel – Interviews & Updates

**ITU** International Telecommunication Union

ITU videos  
itutelecommunication's Channel

Subscribe All Uploads Playlists

« see all uploads

Search

cybersecurity™

WSIS Action Line C5: 3rd Meeting, 22-23  
ituteleco... - 224 views

WSIS Action Line C5: 3rd Meeting, 22-23  
ituteleco... - 60 views

ITU High Level Segment 2008: H.E.  
ituteleco... - 1,919 views

ITU High Level Segment 2008: H.E.  
ituteleco... - 3,359 views

HLS-08: President of Rwanda H.E. Mr.  
ituteleco... - 6,615 views

ITU and Cybersecurity:  
ituteleco... - 944 views

**www.itu.int**  
International Telecommunication Union

0:13 / 1:29

Info Favorite Share Playlists Flag

**ITU and Cybersecurity: Building confidence in the use of ICT**

From: itutelecommunication | April 02, 2008 | 944 views

A fundamental role of the International Telecommunication Union (ITU) is to build confidence and security in the use of information and communication technologies (ICTs). Secretary-General Dr Hamadoun I. Touré explains how children are particularly vulnerable to cyberspace threats and how ITU is taking concrete steps towards curbing the threats and insecurities related to the information society. ... (more info)



# On-Line Cybersecurity Resources: ITU

All the ITU Publications can be found & downloaded from: [www.itu.int](http://www.itu.int)  
(use the titles below as search terms on the ITU Website Home Page)

- 1) ITU – Global Cybersecurity Agenda – HLEG Strategic Report – 2008
- 2) ITU – Cybersecurity Guide for Developing Countries – 2009
- 3) ITU – “BotNet” Mitigation Toolkit Guide – 2008
- 4) ITU – National Cybersecurity/CIIP Self-Assessment Tool – 2009
- 5) ITU – Toolkit for Cybersecurity Legislation – 2010
- 6) ITU – Understanding Cybercrime: A Guide for Developing Countries-2009
- 7) ITU – Technical Security Standards & Recommendations – “X-Series” – including X.509 (PKI), X.805 (Architecture), X.1205 (Threats & Solutions)
- 8) ITU – GCA: Global Cybersecurity Agenda: Summary Brochure – 2010

.....ITU GCA Home Page: [www.itu.int/osg/csd/cybersecurity/gca/](http://www.itu.int/osg/csd/cybersecurity/gca/)



# On-Line Cybersecurity Resources: Other

- 1) UK ACPO Manager's Guide to e-Crime Investigation V1.4 – 2009
  - 2) UK ACPO National e-Crime Strategy – Report 2009
  - 3) UK ACPO Good Practice Guide for Computer-Based Electronic Evidence-2009  
.....UK eCrime Unit WebLink: [www.met.police.uk/pceu](http://www.met.police.uk/pceu)
  - 4) Cybersecurity Strategy of the United Kingdom: Cabinet Office – 2009
  - 5) Guide to NIST Security Documents: US Dept of Commerce – 2009 [www.csrc.nist.gov](http://www.csrc.nist.gov)
  - 6) ISF (Information Security Forum): Standard of Good Practice for InfoSec – 2007  
.....ISF WebLink: [www.securityforum.org](http://www.securityforum.org)
  - 7) CMU: Steps for Creating National CSIRTs – Carnegie Mellon Uni – 2004
  - 8) ENISA: Step-by-Step Approach on How to Set up a CSIRT – 2006
  - 9) ENISA: CERT Exercise Handbook and Training Handbook – 2008  
.....ENISA WebLink: [www.enisa.europa.eu/act/cert/](http://www.enisa.europa.eu/act/cert/)
- .....Most documents referenced during this ITU Cybersecurity Workshop will be found with a focused Google Search for the Publication Title & Responsible Organisation

# \* ITU Cybersecurity Strategy \*

## *"3-Day Workshop Overview"*

<b>S1- Mon: 9:30-11:00</b>  <b>"The Cybersecurity Challenge!..."</b>	<b>S2-Mon: 11:30-13:00</b>  <b>"The Need for Action!"</b>	<b>S3 - Mon:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Cybersecurity Action Plans"</b>	<b>S4 - Mon:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Cybersecurity Action Plans"</b>
<b>S5- Tues: 9:30-11:00</b>  <b>ITU Cyber Agenda: 1</b> <b>"Cybercrime and Legislation"</b>	<b>S6-Tues: 11:30-13:00</b>  <b>ITU Cyber Agenda: 2</b> <b>"Technological Risks and Solutions"</b>	<b>S7 -Tues:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Legislation and Regulations"</b>	<b>S8 -Tues:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Legislation and Regulations"</b>
<b>S9- Wed: 9:30-11:00</b>  <b>ITU Cyber Agenda: 3</b> <b>"Operational Risks and Organisational Structures"</b>	<b>S10-Wed:11:30-13:00</b>  <b>ITU Cyber Agenda: 4&amp;5</b> <b>"Capacity Building and Collaboration"</b>	<b>S11-Wed:14:00-15:30</b> <b>Group Session:</b>  <b>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</b>	<b>S12-Wed:16:00-17:30</b> <b>Group Session:</b>  <b>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</b>



# **\* Group Workshop Session 11 \***

## **“Completing The Sector Cybersecurity 2011 Roadmap”**

- *Task Worksheet* – National & Organisational Cybersecurity Roadmap
  - *Task 1* – Review ALL Materials & Materials from the 3-Day ITU Workshop
  - *Task 2* – Consider Legal, Technical, Organisational, Training & Intl Measures
  - *Task 3* – Review results from Workshop 1 (Action Plan) & Workshop 2 (Laws)
  - *Task 4* – Brainstorm a list of at least 30 to 40 actions for next 12 months
  - *Task 5* – Structure and prioritise actions according to importance & timescale
  - *Task 6* – Start to complete the 12 month Spreadsheet Roadmap Template
  - *Task 7* – Consider each action task duration & logical relationship to others...
  - *Task 8* – Develop a short presentation & slides to support your roadmap

*.....This is by far the most difficult task of this cybersecurity workshop, but its successful completion should be of significant help in the practical realisation of building cybersecurity organisation within your own critical service sector!*





# \* Group Workshop Session 11 \*

## "Completing The National Cybersecurity Roadmap"

*** Jamaican Cybersecurity Roadmap ***															
Cybersecurity Project Activity - Phase 1 - Jan/Feb/March 2011		Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q1 Project Activity -(1)-															
Q1 Project Activity -(2)-															
Q1 Project Activity -(3)-															
Q1 Project Activity -(4)-															
Q1 Project Activity -(5)-															
Q1 Project Activity -(6)-															
Q1 Project Activity -(7)-															
Q1 Project Activity -(8)-															
Q1 Project Activity -(9)-															
Q1 Project Activity -(10)-															
Cybersecurity Project Activity - Phase 2 - April/May/June 2011		Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q2 Project Activity -(1)-															
Q2 Project Activity -(2)-															
Q2 Project Activity -(3)-															
Q2 Project Activity -(4)-															
Q2 Project Activity -(5)-															
Q2 Project Activity -(6)-															
Q2 Project Activity -(7)-															
Q2 Project Activity -(8)-															
Q2 Project Activity -(9)-															
Q2 Project Activity -(10)-															
Cybersecurity Project Activity - Phase 3 - July/Aug/Sept 2011		Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q3 Project Activity -(1)-															
Q3 Project Activity -(2)-															
Q3 Project Activity -(3)-															
Q3 Project Activity -(4)-															
Q3 Project Activity -(5)-															
Q3 Project Activity -(6)-															
Q3 Project Activity -(7)-															
Q3 Project Activity -(8)-															
Q3 Project Activity -(9)-															
Q3 Project Activity -(10)-															
Cybersecurity Project Activity-Phase 4-Oct/Nov/Dec 2011-2012		Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q4 Project Activity -(1)-															
Q4 Project Activity -(2)-															
Q4 Project Activity -(3)-															
Q4 Project Activity -(4)-															
Q4 Project Activity -(5)-															
Q4 Project Activity -(6)-															
Q4 Project Activity -(7)-															
Q4 Project Activity -(8)-															
Q4 Project Activity -(9)-															
Q4 Project Activity -(10)-															
*** Jamaican Cybersecurity Roadmap ***															





# Jamaican Cybersecurity RoadMap

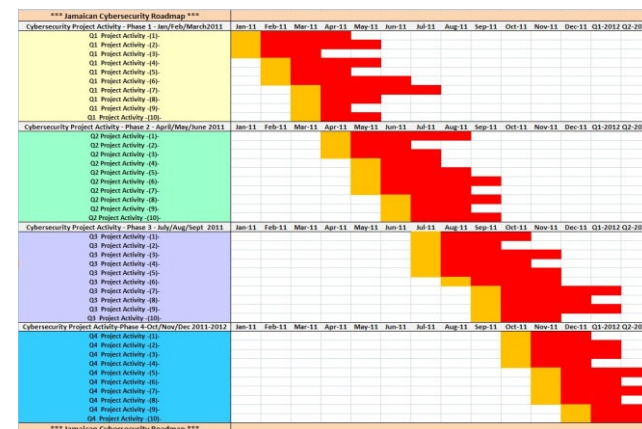
*** Jamaican Cybersecurity Roadmap ***		Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Cybersecurity Project Activity - Phase 1 - Jan/Feb/March 2011															
Q1 Project Activity -(1)- Q1 Project Activity -(2)- Q1 Project Activity -(3)- Q1 Project Activity -(4)- Q1 Project Activity -(5)- Q1 Project Activity -(6)- Q1 Project Activity -(7)- Q1 Project Activity -(8)- Q1 Project Activity -(9)- Q1 Project Activity -(10)-															
Cybersecurity Project Activity - Phase 2 - April/May/June 2011															
Q2 Project Activity -(1)- Q2 Project Activity -(2)- Q2 Project Activity -(3)- Q2 Project Activity -(4)- Q2 Project Activity -(5)- Q2 Project Activity -(6)- Q2 Project Activity -(7)- Q2 Project Activity -(8)- Q2 Project Activity -(9)- Q2 Project Activity -(10)-															
Cybersecurity Project Activity - Phase 3 - July/Aug/Sept 2011															
Q3 Project Activity -(1)- Q3 Project Activity -(2)- Q3 Project Activity -(3)- Q3 Project Activity -(4)- Q3 Project Activity -(5)- Q3 Project Activity -(6)- Q3 Project Activity -(7)- Q3 Project Activity -(8)- Q3 Project Activity -(9)- Q3 Project Activity -(10)-															
Cybersecurity Project Activity-Phase 4-Oct/Nov/Dec 2011-2012															
Q4 Project Activity -(1)- Q4 Project Activity -(2)- Q4 Project Activity -(3)- Q4 Project Activity -(4)- Q4 Project Activity -(5)- Q4 Project Activity -(6)- Q4 Project Activity -(7)- Q4 Project Activity -(8)- Q4 Project Activity -(9)- Q4 Project Activity -(10)-															
*** Jamaican Cybersecurity Roadmap ***															



# Critical Sectors: *Cyber RoadMaps*

Each Critical Service Sector such as Banking, Telecommunications and Energy will require its own Cyber Strategy, Action Plan & Roadmap:

- During this Group Work Sessions we'll work in teams to develop Strategies, Actions and Activities that are relevant for each sector...
- We'll also include actions on the Laws, Policies & Regulations that are required to significantly reduce Cybercrime, Cyber terrorism & Attacks...



**\* Group Workshop Session 11\***  
**Completing the Critical Sector 2011 Roadmap**  
**Suggested Time Allocations for Task Actions: 90mins**

<b>1 – Task Assignment: Choose your Critical Service Sector &amp; Review all Workshop Materials</b>  <i>Government, Banking/Finance Telecomms, Transport, Energy</i>	<b>Task 2 – Consider all the Legal, Technical, Organisational, Training &amp; Intl Measures</b>	<b>Task 3 – Review the Results from previous Workshop Tasks:</b>  <i>(1) Action Plans, and (2) Laws, National Policies &amp; Regulations</i>
<b>Task 4 – Brainstorm at least 30 to 40 Actions for Year-2011</b>	<b>Task 5 – Structure and Prioritise the Actions by Timescale</b>  <i>(Colour-Code Actions by the 2011 Quarter of planned implementation)</i>	<b>Task 6 – Start to Complete the 12 Month Sector RoadMap</b>
<b>Task 7 – Consider &amp; Assign each Action according to its duration and logical project sequence</b>	<b>Task 8 – Prepare Short 10 Min Presentation of 2011 Roadmap</b>	<b>Task 8 – Prepare Short 10min Presentation of 2011 Roadmap</b>

**Note: Each Task Time Segment = 10Mins**

# Key to Cybersecurity Workshop Session

## Colour-Code Classifications: Interactive Tasks

Colour Code Workshop	RED	ORANGE	YELLOW	BLUE	GREEN
<b>Monday</b> <b>-Action Plans -</b>	(1) Legal	(2) Technical	(3) Organisation	(4) Capacity	(5) International
<b>Tuesday</b> <b>- Laws -</b>	Information Disclosure	Computer Misuse	Forgery & ID Fraud	Information Interception	Copyright & Patents Law
<b>Wednesday</b> <b>- Road Map -</b>	<b>Q1-2011</b>	<b>Q2-2011</b>	<b>Q3-2011</b>	<b>Q4-2011</b>	<b>FY2012</b>
<b>Thursday</b> <b>- ICT Security-</b>	Unauthorised Info Access	DDoS-Denial of Services	MALWARE	Disclosure & Misuse	Info Access & Exploitation
<b>Friday</b> <b>- Sector Security -</b>	Cyber Criminal Threat	Cyber Terrorist Threat	Malicious Hacking & Exploitation	Internal Operational Threat	Natural Disaster or Other Event



# \* ITU Cybersecurity Strategy \*

## *"3-Day Workshop Overview"*

<b>S1- Mon: 9:30-11:00</b>  <b>"The Cybersecurity Challenge!..."</b>	<b>S2-Mon: 11:30-13:00</b>  <b>"The Need for Action!"</b>	<b>S3 - Mon:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Cybersecurity Action Plans"</b>	<b>S4 - Mon:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Cybersecurity Action Plans"</b>
<b>S5- Tues: 9:30-11:00</b>  <b>ITU Cyber Agenda: 1</b> <b>"Cybercrime and Legislation"</b>	<b>S6-Tues: 11:30-13:00</b>  <b>ITU Cyber Agenda: 2</b> <b>"Technological Risks and Solutions"</b>	<b>S7 -Tues:14:00-15:30</b> <b>Group Session:</b>  <b>"Developing the National Legislation and Regulations"</b>	<b>S8 -Tues:16:00-17:30</b> <b>Group Session:</b>  <b>"Group Discussion: National Legislation and Regulations"</b>
<b>S9- Wed: 9:30-11:00</b>  <b>ITU Cyber Agenda: 3</b> <b>"Operational Risks and Organisational Structures"</b>	<b>S10-Wed:11:30-13:00</b>  <b>ITU Cyber Agenda: 4&amp;5</b> <b>"Capacity Building and Collaboration"</b>	<b>S11-Wed:14:00-15:30</b> <b>Group Session:</b>  <b>"Working on the Jamaican Cybersecurity Plans &amp; Roadmap"</b>	<b>S12-Wed:16:00-17:30</b> <b>Group Session:</b>  <b>"The Jamaican Cybersecurity Action Plans &amp; Roadmap"</b>



\* **Group Workshop Session 12\***

**Team Discussion: Jamaican Cybersecurity Sector Roadmaps**

**Schedule: Task Presentations = 90mins**

<b>Group 1 = Government Roadmap(15mins)</b>		<b>Group 2 = Banking/Finance Roadmap(15Mins)</b>	
<b>Group 3 = Telecomms/Mobile Roadmap(15Mins)</b>		<b>Group 4 = Transport or Energy Roadmap(15Mins)</b>	
<b>Group Task Discussion (10Mins)</b> <ul style="list-style-type: none"> <li>* Cybersecurity Strategy</li> <li>* Laws, Policies &amp; Regulations</li> <li>* Cybersecurity Organisation</li> <li>* Technologies &amp; Operations</li> <li>* Training &amp; Partnership</li> </ul>		<b>Review On-Line Resources and Next Steps for Personal Study &amp; Research on Cybersecurity</b>	<b>Final Discussion &amp; Wrap-Up</b>



# **\* Group Workshop Session 12 \***

## **Final Group Discussion & Workshop Wrap-Up!**

- 1) Workshop Feedback : Presentation Sessions & Workgroup Tasks
- 2) Review of On-Line Resources & Guidelines for Further Reading
- 3) Final Questions, Discussion and Workshop Wrap-Up!

**.....THANK-YOU!**



# Cybersecurity Workshop: Technologies, Standards & Operations – Back-Up

## BACK-UP SLIDES



University of Technology,  
Jamaica

ITU Centres of Excellence Network for the Caribbean Region  
Developing a National and Organizational Cybersecurity Strategy  
13-15 September, Kingston, Jamaica



International  
Telecommunication  
Union

Committed to connecting the world

# Key to Cybersecurity Workshop Session

## Colour-Code Classifications: Interactive Tasks

Colour Code Workshop	RED	ORANGE	YELLOW	BLUE	GREEN
<b>Monday</b> <b>-Action Plans -</b>	(1) Legal	(2) Technical	(3) Organisation	(4) Capacity	(5) International
<b>Tuesday</b> <b>- Laws -</b>	Information Disclosure	Computer Misuse	Forgery & ID Fraud	Information Interception	Copyright & Patents Law
<b>Wednesday</b> <b>- Road Map -</b>	Q1-2011	Q2-2011	Q3-2011	Q4-2011	FY2012
<b>Thursday</b> <b>- ICT Security-</b>	Unauthorised Info Access	DDoS-Denial of Services	MALWARE	Disclosure & Misuse	Info Access & Exploitation
<b>Friday</b> <b>- Sector Security -</b>	Cyber Criminal Threat	Cyber Terrorist Threat	Malicious Hacking & Exploitation	Internal Operational Threat	Natural Disaster or Other Event

