A Report on Cybercrime Laws in the Caribbean

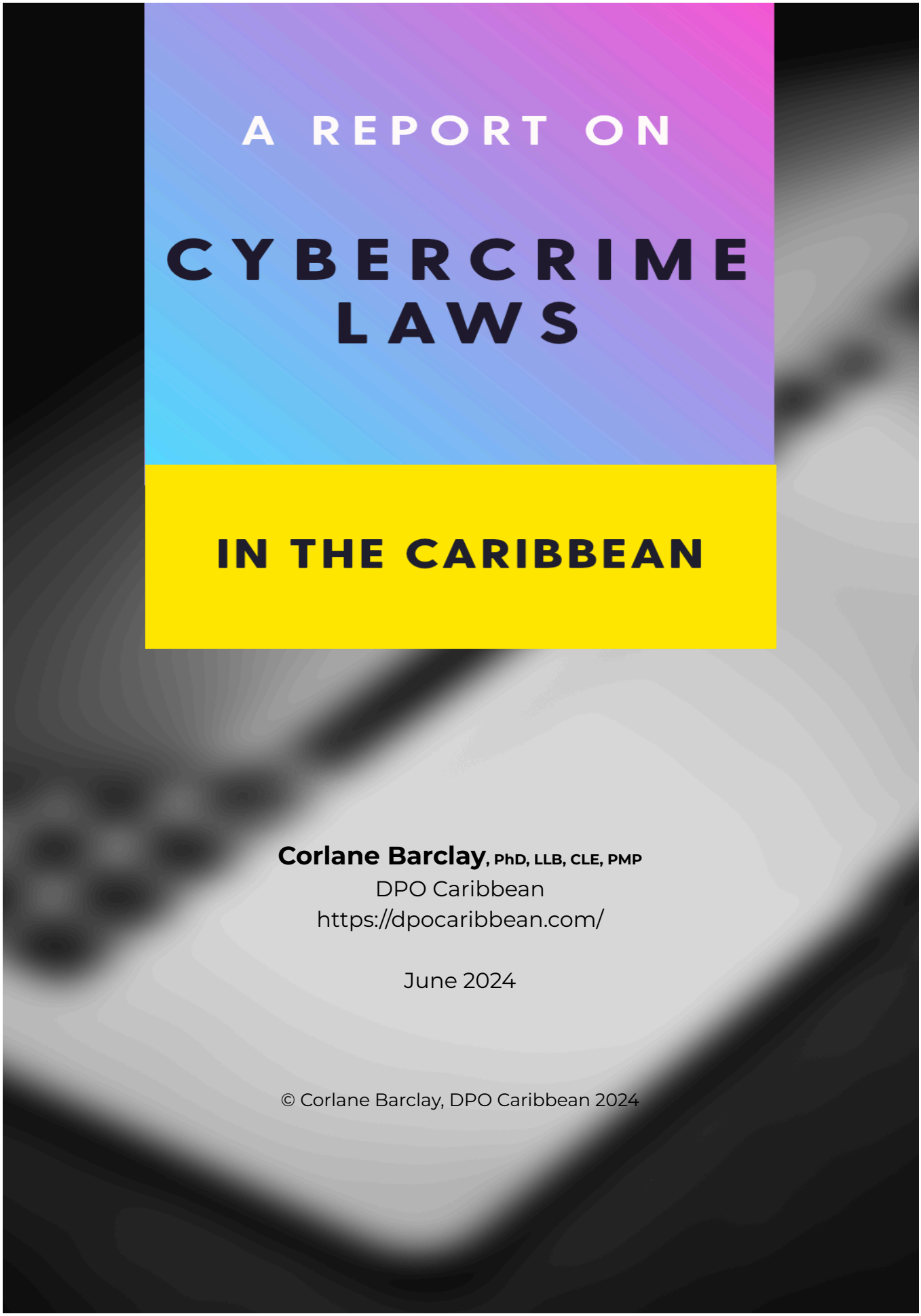
Technical Report · June 2024

DOI: 10.13140/RG.2.2.13491.85285

1 author:

Corlane Barclay
DPO Caribbean
66 PUBLICATIONS **577** CITATIONS

SEE PROFILE



A REPORT ON

CYBERCRIME LAWS

IN THE CARIBBEAN

Corlane Barclay, PhD, LLB, CLE, PMP
DPO Caribbean
https://dpocaribbean.com/

June 2024

Table of Contents

Introduction....3
Cybercrime Law Developments: Regional Snapshot....3
National Cybercrime Laws....8
1. Anguilla....8
2. Antigua and Barbuda....8
3. Bahamas....9
4. Barbados....9
5. Belize....10
6. Bermuda....11
7. British Virgin Islands....12
8. The Cayman Islands....13
9. Dominica....13
10. Grenada....14
11. Guyana....14
12. Haiti....15
13. Jamaica....15
14. Montserrat....16
15. Saint Kitts and Nevis....17
16. Saint Lucia....17
17. Saint Vincent and the Grenadines....18
18. Suriname....19
19. Trinidad and Tobago....19
20. Turks and Caicos Islands....20
Conclusion....20

Introduction

Cybercrime or computer-related crimes continue to be an existential threat in today's world. In the Caribbean, our Regional Cybersecurity Threat Report highlighted some of the top threats in the region such as ransomware, social engineering attacks such as phishing, data breaches, card fraud, business email compromise, and more. These forms of criminal acts are rapidly evolving in sophistication, scale and intensity as a result of the development of more advanced threat service models, increased vulnerabilities of individual, organisational and state targets, and the exploitation of the use of artificial intelligence and other emerging technologies. As economies grapple with finding tools, measures, and solutions, legal measures have been shown to be a reliable approach to managing the evolving nature of this form of transnational crime. It is therefore crucial that countries take a proactive approach in establishing a robust legal platform to efficiently and effectively enforce the evolving nature of cybercrime.

The purpose of this report is to map the principal cybercrime laws of key countries in the Caribbean. The report focuses on the 20 CARICOM member and associate member states.

Cybercrime Law Developments: Regional Snapshot

In respect of the Caribbean, we show a mapping of each country's Global Cybersecurity Index score, the status of adoption of cybercrime law, and the state of membership to the Budapest Convention on Cybercrime.

The ITU Global Cybersecurity Index (GCI) measures a country's commitment to cybersecurity at the global level. The latest version (2021) of the GCI highlighted that countries in the Caribbean are ranked comparatively low across the 5 pillars consisting of legal measures, technical measures, organisational measures, capacity development and cooperation measures. The stark reality forced us to ask the question as to whether the Caribbean Community is committed to cybersecurity.

Despite the relatively low cybersecurity maturity of countries in the region, the cybercrime legal profiles of these countries reflect that some level of priority is placed on the development and implementation of laws to combat cybercrime. The scores relating to legal measures further demonstrate that

the legal pillar accounts for a significant portion of the overall score of many countries in the Caribbean.

The Budapest Convention on Cybercrime is currently the sole global framework that provides for the criminalisation of cybercrime, procedural powers to secure electronic evidence and a legal basis for international cooperation. With over 70 parties to the Budapest Convention on Cybercrime, any state may accede, subject to the procedure set out in Article 37. However, this option has not been actively leveraged in the Caribbean.

Regional Overview:

- 16/20 countries have a basic cybercrime legal framework
- 18/20 countries have no formal relationship with the Budapest Convention on Cybercrime
    - 1 country is a party to the Budapest Convention on Cybercrime: Grenada joined in 2024
    - 1 country is a signatory and invited to accede to the Budapest Convention on Cybercrime: Trinidad and Tobago
- In many instances, a significant portion of countries' GCI scores can be attributed to legal measures
- Despite the heavy reliance on legal measures, opportunities exist for further development of this pillar and other areas in the wider ecosystem

Table: GCI Scores and Adoption of Cybercrime Laws

Country	GCI Score (2021): (x/100)	GCI Score: Legal Measures: (x/20)	Contribution of legal measures to country commitment to cybersecurity	Adoption of Cybercrime Law	Party to Budapest Convention on Cybercrime
Anguilla	n/a	n/a	n/a	No	No
Antigua and Barbuda	15.62	11.36	72.73%	Yes	No
Bahamas	13.37	12.85	96.11%	Yes	No

Country	GCI Score (2021): (x/100)	GCI Score: Legal Measures: (x/20)	Contribution of legal measures to country commitment to cybersecurity	Adoption of Cybercrime Law	Party to Budapest Convention on Cybercrime
Barbados	16.89	12.63	74.78%	Yes	No
Belize	10.29	5.77	56.07%	Yes	No
Bermuda	n/a	n/a	n/a	Yes	No
British Virgin Islands	n/a	n/a	n/a	Yes	No
Cayman Islands	n/a	n/a	n/a	Yes	No
Dominica	4.2	0.85	20.24%	No	No
Grenada	9.41	9.41	100.00%	Yes	Yes
Guyana	28.11	13.12	46.67%	Yes	No
Jamaica	32.53	11.54	35.47%	Yes	No
Haiti	6.4	0.85	13.28%	No	No
Montserrat	n/a	n/a	n/a	Yes	No
St. Kitts and Nevis	12.44	5	40.19%	Yes	No
Saint Lucia	10.96	6.7	61.13%	Yes	No
St. Vincent and the Grenadines	12.18	10.95	89.90%	Yes	No
Suriname	31.2	11.13	35.67%	Yes	No
Trinidad and Tobago	22.18	7.94	35.80%	Yes	Signed and invited to accede
Turks and Caicos	n/a	n/a	n/a	No	No

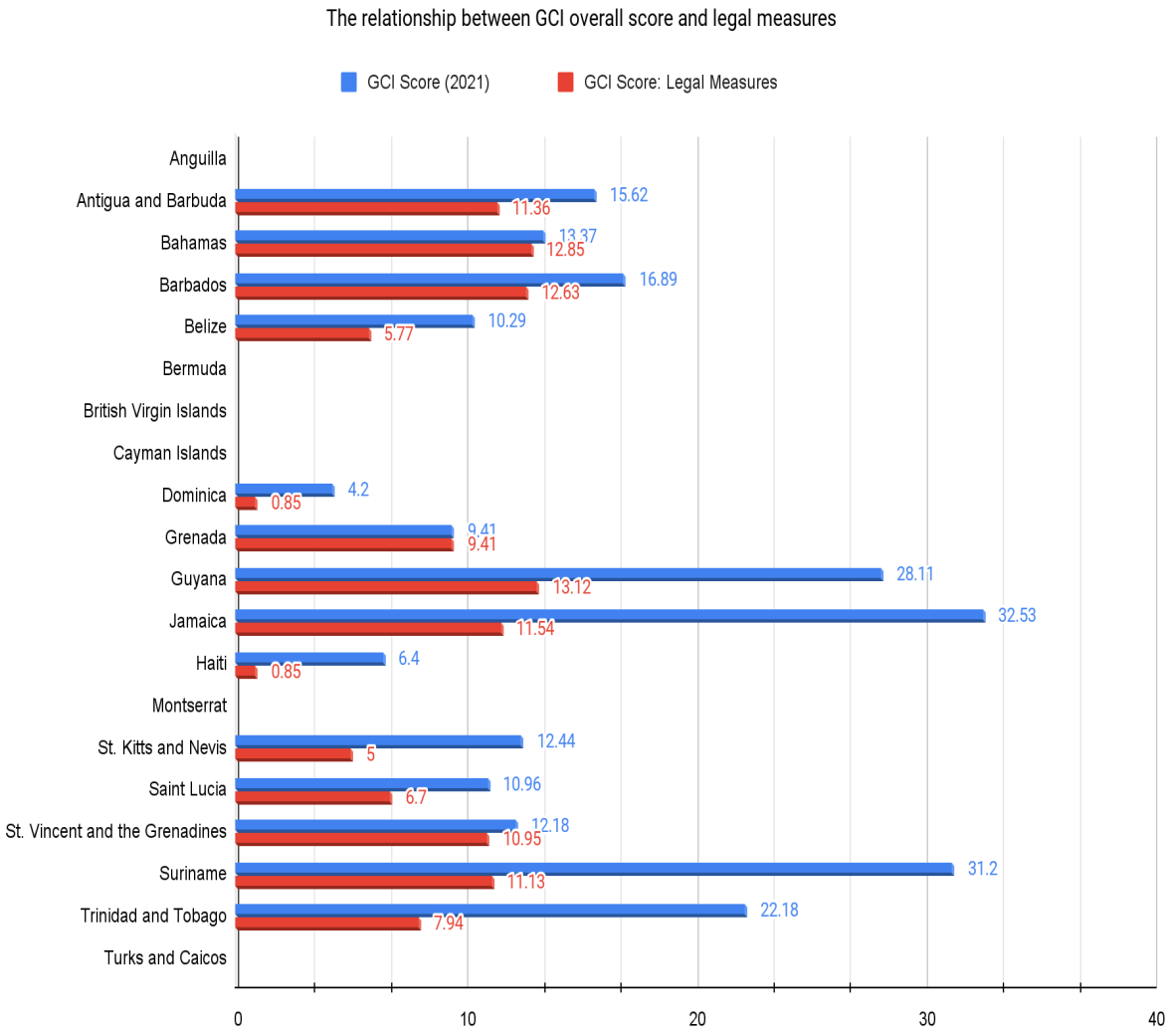


Figure 1: The relationship between GCI overall score and legal measures

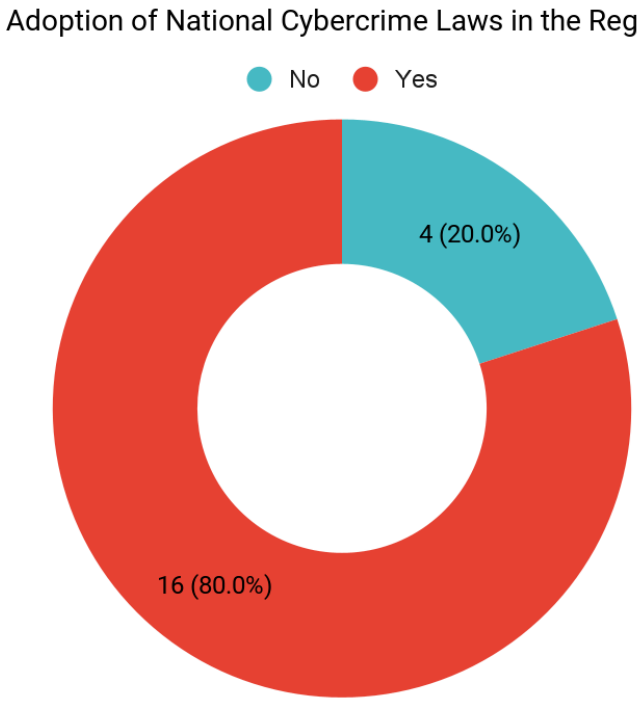


Figure 2: Adoption of national cybercrime laws in the Caribbean

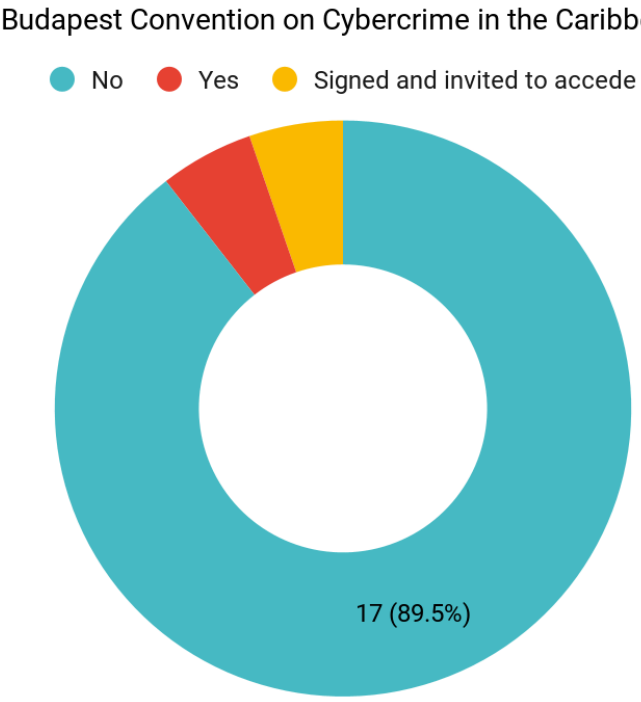


Figure 3: Budapest Convention of Cybercrime in the Caribbean

National Cybercrime Laws

1. Anguilla

No substantive national cybercrime law was identified. The Criminal Code of Anguilla provides a basic legal framework for certain offences.

2. Antigua and Barbuda

Cybercrime Legal Framework
Antigua and Barbuda Electronic Crimes Act, 2013
Electronic Crimes (Amendment) Act, 2018

Substantive criminal provisions
The Electronic Crimes Act provides for the prevention and punishment of electronic crimes and related matters. Cybercrime offences include access and interference, sending offensive messages, identity theft, electronic forgery, electronic fraud, violation of privacy, misuse of encryption, child pornography, electronic terrorism, harassment, false websites and spam.

Penalties and sanctions
The Act provides for several measures:

- A person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.
- Under section 28, extradition may be granted or obtained pursuant to the Extradition Act.
- An order for compensation may be granted for damage caused to a person's electronic system, program or data by the offence in respect of which the sentence is passed.
- In addition to any penalty imposed, according to section 30, the Court may order the forfeiture of any apparatus, article or thing which is the subject matter of the offence or is used in connection with the commission of the offence, including any obscene matter.
- In addition, the Court may make an order that an obscene matter be deleted from or no longer stored or made available through an electronic system.

Procedural measures and law enforcement
The Act provides for measures such as preservation orders, production orders, access, search and seizure for the purpose of investigation, real-time collection of traffic data, and mobile phone tracking in emergencies.

3. Bahamas

Cybercrime Legal Framework
Bahamas Computer Misuse Act, 2003

Substantive criminal provisions
The Computer Misuse Act makes provisions for securing computer material against unauthorised access or modification and for connected purposes. Cybercrime offences include unauthorised access, access with intent, unauthorised modification, unauthorised use or interception, unauthorised obstruction, and unauthorised disclosure of access code.

Penalties and sanctions
The Act provides for several measures:

- A person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.
- Under section 17, the court may order that property to be forfeited to the Crown where the property has been used for the purpose of committing or facilitating the commission of, the offence in question
- The court may also make an order for a payment by way of compensation for any damage caused to the person's computer, program or data as a result of the offence for which the sentence is passed.

Procedural measures and law enforcement
The Act provides for measures such as saving for investigations relating to powers conferred under any written law, police powers, and the power of police officers to access computers and data.

4. Barbados

Cybercrime Legal Framework
Barbados Computer Misuse Act, 2005

Barbados Cybercrime Bill, 2024

Substantive criminal provisions
The Computer Misuse Act provides for the protection of computer systems and the information contained in those systems from unauthorised access, from abuse by persons authorised to have access, and for related matters. Cybercrime offences include illegal access, interfering with data, interfering with a computer system, illegal interception of data, illegal devices, access with intention, child pornography, and malicious communications.

The Cybercrime Bill is to replace the Computer Misuse Act and is currently before the Joint Select Committee. The Bill provides for similar offences as the existing law while providing for additional offences such as offences relating to critical information infrastructure systems, computer-related forgery, computer-related fraud, child grooming, cyberbullying, and cyberterrorism.

Penalties and sanctions
The Act provides for several measures:

- A person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.
- Under section 21, the court may also make an order for a payment by way of compensation for any damage caused to the person's computer, program or data as a result of the commission of an offence for which a sentence is passed.

Procedural measures and law enforcement
The Act provides for measures such as search and seizure, production of data for criminal proceedings, and preservation of data for criminal proceedings.

5. Belize

Cybercrime Legal Framework
Belize Cybercrime Act, 2020

Substantive criminal provisions
The Cybercrime Act seeks to combat cybercrime by creating offences of cybercrime, to provide for penalties, investigation and prosecution of the offences of cybercrime, and connected matters. Cybercrime offences include

illegal access, illegal data interference, illegal system interference, illegal devices and codes, computer-related forgery, identity-related fraud and theft, child luring, publication or transmission of images, using a computer system to harass a person, infringement of copyright, etc.

Penalties and sanctions
The Act provides for several measures:

- A person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.
- The court may grant a compensation order, upon application, if it is determined that the applicant's pain and suffering, loss, harm or injury is caused by the commission of an offence under the Cybercrime Act.
- Under section 33, the court may order that any property used for or in connection with the commission of an offence, or obtained as a result of or in connection with, the commission of the offence, be forfeited to the State.
- According to section 39, the offences described under the Cybercrime Act are deemed to be extraditable offences where the Extradition Act applies.

Procedural measures and law enforcement
The Cybercrime Act provides for measures such as search and seizure, production order, expedited preservation order, forfeiture order, mutual legal assistance, and transborder access to computer data with consent or when unsecured and publicly available.

6. Bermuda

Cybercrime Legal Framework
Bermuda Computer Misuse Act, 2024

Substantive criminal provisions
The Computer Misuse Act repeals the previous law and provides for criminal offences relating to unauthorised access to computers. Cybercrime offences include unauthorised access to computer material, unauthorised access with intent, unauthorised acts with intent to impair, or with recklessness as to impairing, operation of a computer, unauthorised acts causing, or creating

the risk of, serious damage, making, supplying or obtaining articles for use in committing an offence under the Act.

Penalties and sanctions
The Act provides for several measures:

- A person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.
- The court may order that property to be forfeited to the Crown in accordance with section 15.

Procedural measures and law enforcement
The Act provides for measures associated with police powers as described in section 14.

7. British Virgin Islands

Cybercrime Legal Framework
BVI Computer Misuse and Cybercrime Act, 2014

Substantive criminal provisions
The Computer Misuse and Cybercrime Act provides for securing computer material and prohibits the unauthorised access, modification or any form of interference with such material or the misuse of computers and makes provision for other matters connected thereto. Other offences include unauthorised disclosure of passwords, access codes, unlawfully making available devices or data, offences involving protected computers, unlawful publication of computer data and child pornography, and using a computer for child pornography.

Penalties and sanctions
The Act provides for several measures:

- A person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.
- Under section 17, the court may, in addition to any penalty imposed on the person convicted, order that person to pay a fixed sum as

compensation to any person who has suffered loss as a result of the commission of the offence.

Procedural measures and law enforcement
No specific procedural or law enforcement measure is contemplated in the Act.

8. The Cayman Islands

Cybercrime Legal Framework
The Cayman Islands Computer Misuse Law (2015 Revision)

Substantive criminal provisions
The Computer Misuse Law provides for computer-related offences. Cybercrime offences include unauthorised access to computer material, unauthorised access with intent to commit or to facilitate the commission of further offences, unauthorised modification of computer material, unauthorised use or interception of computer service, causing a computer to cease to function.

Penalties and sanctions
The Law provides for several measures:

- A person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.
- The court may make an order for the payment of a sum by way of compensation to any person for any damage caused to the person's computer or information by the offence for which the sentence is passed.
- The court may order that property to be forfeited to the Crown pursuant to section 14.

Procedural measures and law enforcement
The Act provides for measures associated with police powers described in section 13.

9. Dominica

No substantive national cybercrime law was identified.

10. Grenada

Cybercrime Legal Framework
Grenada Electronic Crimes Act, 2013

Substantive criminal provisions
The Act provides for the prevention and punishment of electronic crimes. Offences include unauthorised access and interference, sending offensive messages through communication services, identify theft, electronic forgery, electronic fraud, violation of privacy, misuse of encryption, child pornography, sensitive electronic system, electronic terrorism, prank calls to law enforcement, electronic stalking, spoof and spam, unauthorised access to code.

Penalties and sanctions
The Act provides for several measures:

- A person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.
- A court may make an order for the payment of the sum of money fixed by way of compensation to a person for damage caused to that person's electronic system, program or data by an offence in respect of which the sentence is passed.
- In addition to any penalty imposed, a court may order the forfeiture of any apparatus, article or thing which is the subject matter of the offence or is used in connection with the commission of the offence.
- According to section 30, any offence under Part II of the Act is considered to be an extraditable crime for which extradition may be granted or obtained under the Extradition Act Cap. 98.

Procedural measures and law enforcement
The Law provides for measures such as a preservation order, production order, real-time collection of traffic data, and mobile phone tracking in emergencies.

11. Guyana

Cybercrime Legal Framework
Guyana Cybercrime Act, 2018

Substantive criminal provisions
The Act seeks to combat cybercrime by creating certain offences and to provide for penalties, investigations and prosecution of offences. Cybercrime offences include illegal access, illegal interception, illegal data interference, illegal acquisition of data, illegal system interference, illegal devices, computer-related forgery, computer-related fraud, offences affecting critical infrastructure, identity-related offences, child pornography, and child luring.

Penalties and sanctions
The Act provides for several measures:

- A person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.
- A court may make an order for the payment of the sum of money fixed by way of compensation to a person for damage caused to that person's electronic system, program or data by an offence in respect of which the sentence is passed.
- Where the court finds that a person has suffered loss or damage because of the commission of an offence, the court may order the person convicted to pay a fixed sum as compensation.
- The court may order the forfeiture of any property used for or in connection with the commission of the offence pursuant to section 40.

Procedural measures and law enforcement
The Act provides for measures such as a production order, expedited preservation, and disclosure of traffic data.

12. Haiti

No substantive national cybercrime law was identified.

13. Jamaica

Cybercrime Legal Framework
Jamaica Cybercrimes Act, 2015

Substantive criminal provisions
The Act creates cybercrime offences and penalties. Cybercrime offences include unauthorised access, access with intent, unauthorised modification, unauthorised interception, unauthorised obstruction of operation of computer, computer-related fraud or forgery, use of computer for malicious communication, unlawfully making available devices or data for the commission of offence, offences relating to protected computers.

Penalties and sanctions
The Act provides for several measures:

- A person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.
- The court may order the forfeiture of the computer material used in the commission of the offence pursuant to section 20.

Procedural measures and law enforcement
The Act provides for measures such as the preservation of data, production orders, and search and seized warrants.

14. Montserrat

Cybercrime Legal Framework
Montserrat Penal Code (Amendment) Act, 2022

Substantive criminal provisions
The Act creates cybercrime offences. Cybercrime offences include unauthorised access, unauthorised acts with intent, offences affecting critical infrastructure, computer-related forgery, computer-related fraud, sending letter, electronic communication or article with intent to cause distress or anxiety, improper use of public electronic communications network, and offence by body corporate.

Penalties and sanctions
The Act provides that a person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.

Procedural measures and law enforcement
No specific procedural or law enforcement measure is provided for in the Act.

15.Saint Kitts and Nevis

Cybercrime Legal Framework
Saint Kitts and Nevis Electronic Crimes Act, 2017

Substantive criminal provisions
The Act prohibits certain acts. Cybercrime offences include illegal access, illegal remaining, interfering with data, interfering with a computer system, illegal interception, possession, sale, etc. of illegal devices, computer-related fraud, unlawful disclosure of access code, unauthorised access to a restricted computer system, child pornography, unlawful communications, computer-related forgery, data espionage, identity-related crimes, spam.

Penalties and sanctions
The Act provides that a person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.

Procedural measures and law enforcement
The Act provides for measures such as production orders, and expedited preservation of computer data.

16. Saint Lucia

Cybercrime Legal Framework
Saint Lucia Computer Misuse Act 2009

Substantive criminal provisions
The Act seeks to protect the integrity of computer systems. Cybercrime offences include unauthorised access, access with intent, unauthorised access to and interception, unauthorised modification, damaging and denying access to computer systems, unauthorised disclosure of passwords, unlawful possession of devices and data, electronic fraud, offences related to protected computer systems, indecent photographs of children, malicious communication.

Penalties and sanctions
The Act provides for several measures:

- A person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.
- Section 23 specifies that the court may make an order against a person convicted for the payment of a sum by way of compensation to any person for any damage caused to the person's computer systems, program, or data by the offence in respect of which the sentence is passed.
- Under section 24, the court may make an order for the forfeiture of any apparatus, article or thing which is the subject matter of the offence or is used in connection with the commission of the offence.

Procedural measures and law enforcement
The Act provides for measures such as preservation orders, production orders, and collection of traffic data.

17. Saint Vincent and the Grenadines

Cybercrime Legal Framework
Saint Vincent and the Grenadines Cybercrime Act, 2016

Substantive criminal provisions
The Act provides for offences relating to cybercrimes. Cybercrime offences include illegal access, illegal remaining, illegal interception, illegal data interference, illegal acquisition of data, illegal system interference, offences affecting critical infrastructure, illegal devices, identity-related crimes, computer-related forgery, computer-related fraud, child pornography, violation of privacy, spam, spoofing.

Penalties and sanctions
The Act provides for several measures:

- A person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.
- The court may make an order for payment of compensation pursuant to section 30.

- The court may make an order for any property to be forfeited to the Crown in accordance with section 31.
- Section 39 specifies certain extraditable offences for which extradition may be granted under the Fugitives Offenders Act.

Procedural measures and law enforcement
The Act provides for measures such as expedited preservation, disclosure of traffic data, collection of traffic data, and search and seizure.

18. Suriname

Cybercrime Legal Framework
Suriname Criminal Code

Substantive criminal provisions
The Code provides for certain offences relating to cybercrime. Cybercrime offences include illegal access, disruption of a computer data/computer system, computer-related forgery and fraud, offences related to child pornography, and misuse of technical tools.

Penalties and sanctions
The Act provides that an offence is punishable by fine or imprisonment for a specified term.

Procedural measures and law enforcement
No procedural powers are identified in the Criminal Code.

19. Trinidad and Tobago

Cybercrime Legal Framework
Trinidad and Tobago Computer Misuse Act, 2000
Trinidad and Tobago Cyber Crime Bill, 2017

Substantive criminal provisions
The Act prohibits unauthorised access, use or interference with a computer. Cybercrime offences include unauthorised access, access with intent, unauthorised modification, unauthorised use or interception, unauthorised obstruction, unauthorised disclosure of access code, offences involving

protected computers, unauthorised receiving or giving access, causing a computer to cease to function.

Penalties and sanctions
The Act provides for several measures:

- A person who is guilty of the offence is liable on summary conviction or conviction on indictment to a fine or imprisonment for a specified term, or both.
- The court may make an order for payment of compensation pursuant to section 14.

Procedural measures and law enforcement
The Act provides for measures such as the power of a police officer to access computer programs or data.

20. Turks and Caicos Islands

No substantive national cybercrime law was identified.

Conclusion

This report on cybercrime laws in the Caribbean adds to the global dialogue relating to cyber risks and cybercrime measures, particularly as it relates to the Caribbean and its commitment to combating cybercrime and building capacities and capabilities in cybersecurity.

Cyber laws and regulations are commonly perceived as an effective method of reducing cyber risks. It is important therefore that countries prioritise the development, implementation and use of appropriate legal frameworks to combat cybercrime. The report centres on the principal cybercrime laws of 20 countries in the Caribbean. Future reports will cast a wider net and focus on the broader cybercrime legal framework that contemplates other related laws in addition to the principal cybercrime law of each country.

The mapping highlights that many countries in the region have a relatively sound basic legal framework for cybercrime. Several countries such as Barbados and Bermuda have recently passed new cybercrime laws or are in an advanced stage of passing new or amended laws. Key substantive law

measures present in many jurisdictions include child online protection, offences relating to online harassment, unauthorised access and modification, intellectual property breaches, attempt, aiding, and abetting. Common sanctions include fines, imprisonment, forfeiture, compensation for loss and damage as a result of the commission of an offence and extraditable offences. Procedural measures include search and seizure, production orders, expedited preservation, and real-time collection of traffic data.

Despite this state of progress in the region, there are opportunities for further improvements in terms of closer alignment of the substantive criminal and procedural law, and cooperation measures with the Budapest Convention on Cybercrime, increased use and enforcement of existing laws and the identification of appropriate mechanisms for addressing emerging cyber risks.

About DPO Caribbean

DPO Caribbean provides expert advisory, legal and technical support in cybersecurity, data protection and privacy to public and private entities to meet their policy and legislative agendas and regulatory compliance obligations and requirements.