2021 Caribbean Cyber Security and Privacy (CSPR) Report

Released: October 2, 2020.

g5cybersecurity.com

Table of Contents

In September 2020, we analysed 13,791 websites belonging to businesses and people in the Caribbean and measured the level of national progress in Cyber Security and Data Protection to give you real and useful statistics.

G5 Cyber Security

13, 791 websites analysed across 32 countries and territories

Anguilla - 212
Antigua and Barbuda - 141
Aruba - 677
Bahamas - 169
Barbados - 973
Belize - 550
Bermuda - 541
Bonaire, St. Eustatius and Saba - 56
British Virgin Islands - 176
Cayman Islands - 1055
Cuba - 355
Curaçao - 339
Dominica - 165
Dominican Republic - 761
Grenada - 481
Guadeloupe - 156
Guyana - 289
Haiti - 198
Jamaica - 2244
Martinique - 60
Montserrat - 50
Puerto Rico - 2095
St. Barthélemy - 51
St. Kitts and Nevis - 233
St. Lucia - 335
St. Maarten - 153
St. Martin - 80
French Antilles Government - 189
St. Vincent and the Grenadines - 194
Suriname - 178
Trinidad and Tobago - 195
The Turks and Caicos Islands - 262
US Virgin Islands - 178

What is this Report?

This report is an analysis of Cyber Security and Data Privacy relating to websites and businesses operating in the Caribbean. This report is divided into several sections.

G5 Cyber Security provides Cyber Security and Data Privacy services to businesses internationally.

32

Countries and territories covered from the Caribbean

13,791

Websites analysed.

43m+

Citizens affected.

The Purpose of this Report

This report is intended to be used for educational purposes. However, we welcome other perspectives on how our report can be used for good.

Visit us at g5cybersecurity.com.

1. **Raise awareness**

   We want everyone to appreciate the importance of Cyber Security & Privacy.

2. **Provide reliable local data**

   We want the Caribbean to have reliable data they can trust to make decisions.

3. **Create opportunities**

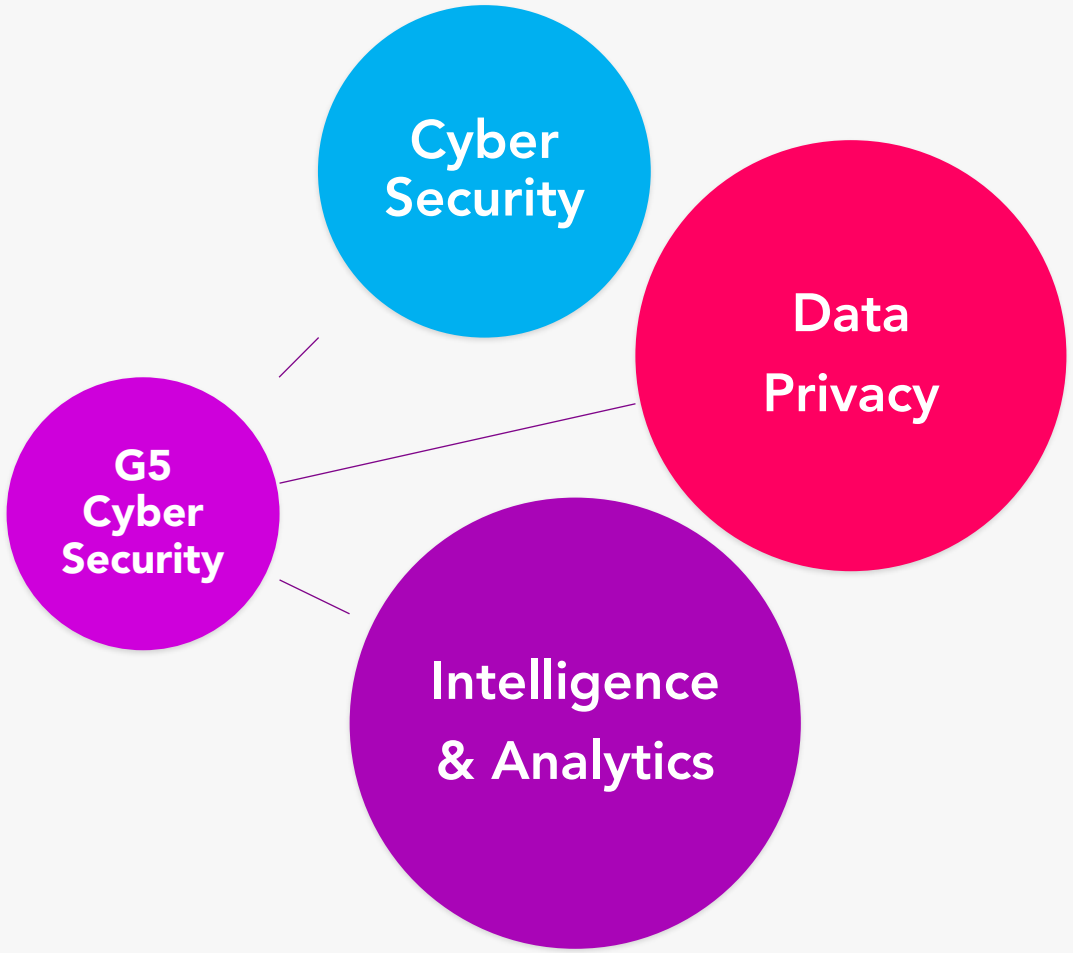
   We want to create more opportunities for professionals and businesses.

About the Lead Researcher

Gavin Dennis CISSP, CISM, CASP, CySA+, eWPT

Gavin is an internationally experienced Cyber Security Professional, originally from Jamaica and has over twelve (12) years experience combined across multiple industries. He leads G5 Cyber Security Inc., The Caribbean Cyber Security and Privacy Association (CSPA) Ltd and The G5 Cyber Security Foundation Ltd.

What We Do at G5 Cyber Security, Inc.



Cyber Security services

We protect our clients from Cyber attacks.

Data Privacy services

We protect our clients from data privacy breaches.

Intelligence and Analytics services

We use our data to help businesses and people make smarter decisions.

Our Leadership

Gavin Dennis

Director

Gavin Dennis is the Director of Strategy, Operations and People. Throughout his career, Gavin has worked with several audit firms and supported clients in Europe, Asia, Africa and the Caribbean.

Atasha Bernard

Director

Atasha Bernard has over twelve (12) years experience in auditing, accounting and management providing oversight in financial management, corporate governance and strategic planning.

Supporting Clients Internationally

- No matter where in the world you are, we can support your business remotely.
- Our team is internationally experienced.
- Our team is highly qualified and diverse.
- Upgrade your security vendor, work with us.
- Get 7-day help desk support for your questions.

Book a meeting online today, click here.

Business Partners

We work with companies across the world to delivery premium support to all our clients.

Our partners help to make Cyber Security and Privacy services accessible no matter where our clients are in the world. Learn more at g5cybersecurity.com/partners

It's easy to start working with us

Step – 1

Request a meeting.

We'll meet with you online to understand your requirements

Step – 2

Get a Proposal.

We'll email you a proposal outlining the engagement, costs and timelines.

Step – 3

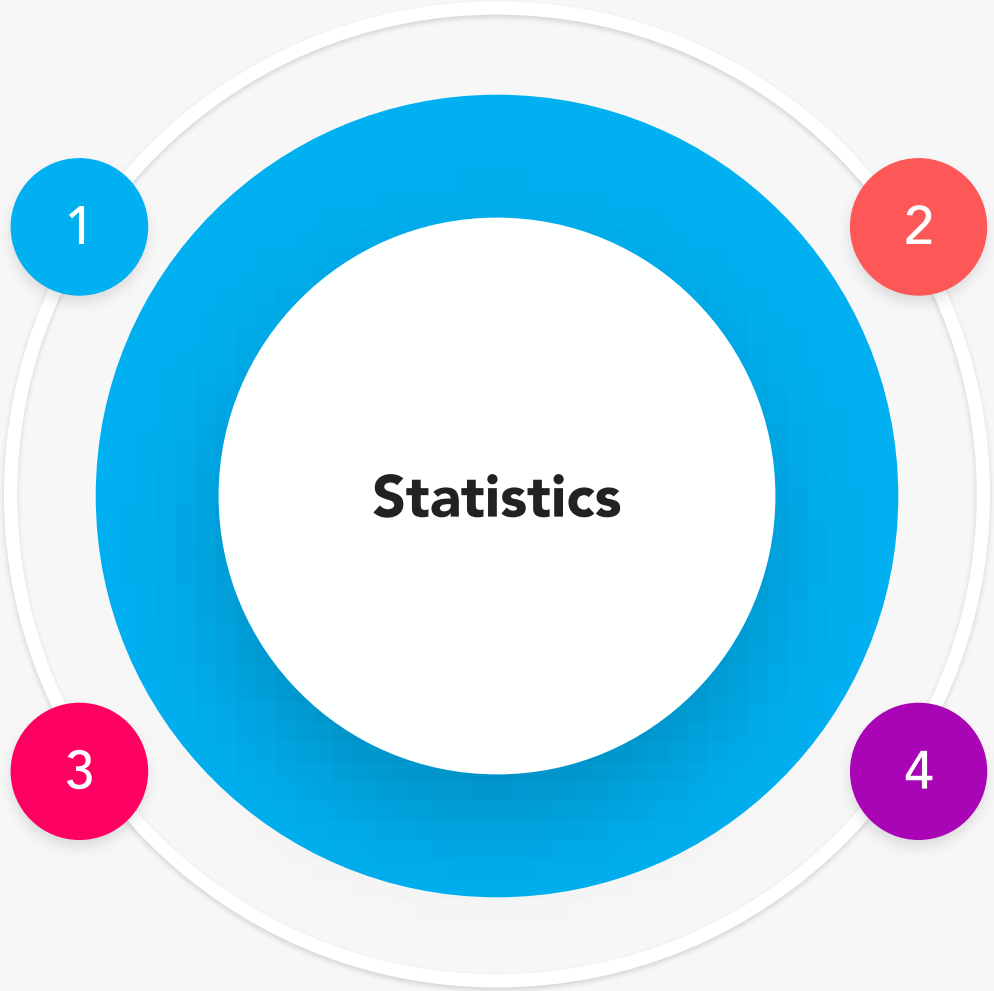
Execute.

We'll execute your requirements and submit the agreed deliverables.

Step – 4

Implement and Improve.

Improve your security and privacy through our continuous support.



1. The **Statistics** sections start here.

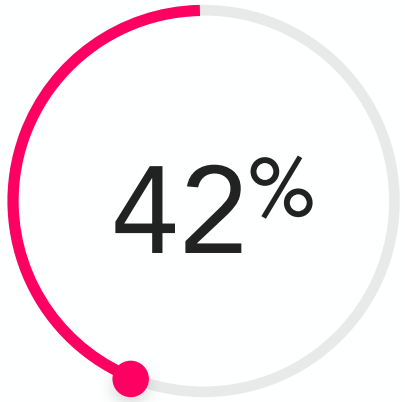
2. All metrics are independently verifiable.

3. You can register HERE to see data samples monthly.

4. Contact us for Cyber Security and Privacy services. Click HERE.

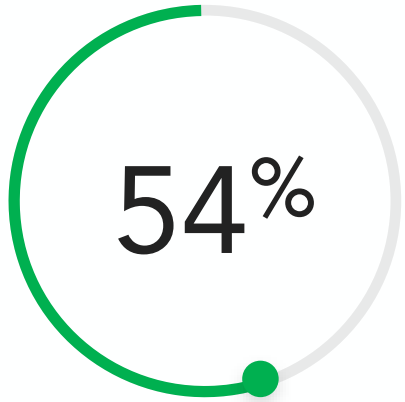
Executive Findings – Technology

High-level details for management professionals.



of domains have related credentials in a data breach.

- Very bad



of websites automatically load over HTTPS

- Positive

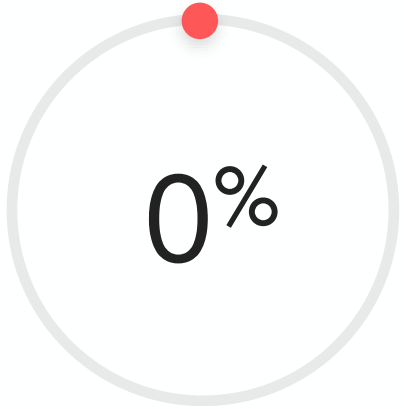
of websites set all expected Security Headers.

- Poor

Executive Findings – National Cyber Security Plans/Strategies

of countries have a documented National Cyber Security Plan

- Positive but poor



of the remaining countries have announced a draft.

- Poor

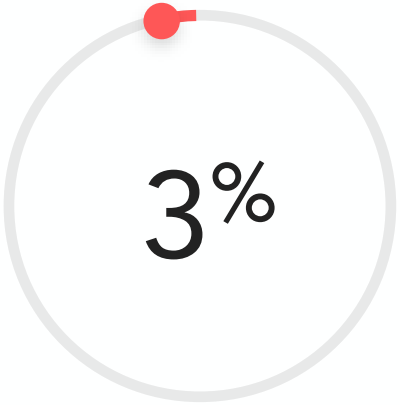
countries are without a National Cyber Security Plan

- Poor

Executive Findings – Cyber Crime Laws

of countries have a Cyber Crime Law

- Positive but poor



of the remaining countries have announced a draft.

- Poor

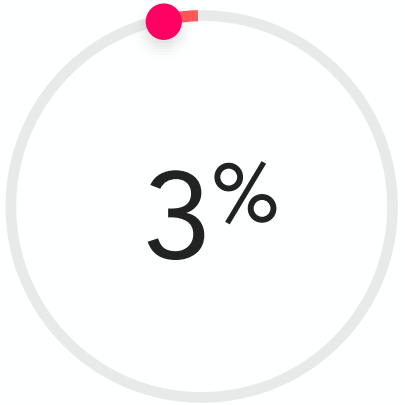
of countries are without a National Cyber Security Plan

- Poor

Executive Findings – National Cyber Incident Response Teams

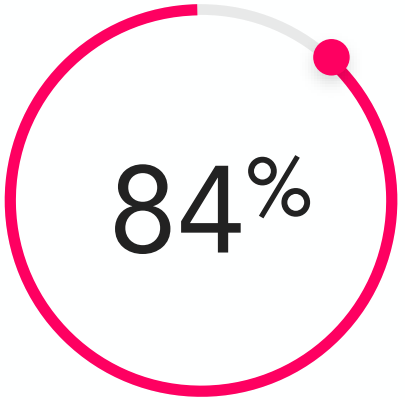
of countries have a National Cyber Incident Response Team

- Positive but poor



of the remaining countries have announced they will start a team

- Poor



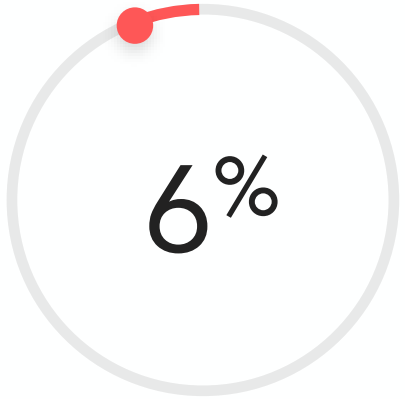
of countries are without a National Cyber Incident Response Team

- Poor

Executive Findings – Data Protection Laws

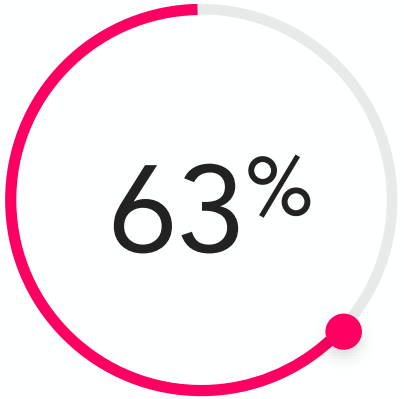
of countries have a Data Protection Law

- Positive but poor



of the remaining countries have announced a draft

- Poor



of countries are without a Data Protection Law

- Poor

Critical Takeaways Governments

Some aspects of the data that stood out that we believe you should know.

5,998

government credentials were identified in data dumps on the infamous dark web.

58%

of government websites do not automatically load over HTTPS, 42% do.

93%

of government websites do not set expected Security Headers, 7% do.

Critical Takeaways
Information Technology (IT) businesses

Some aspects of the data that stood out that we believe you should know.

93,273

credentials of IT businesses were identified in data dumps on the dark web.

37%

of all IT business websites do not automatically load over HTTPS, 63% do.

81%

of IT business websites do not set expected Security Headers, 19% do.

Operational Roadmap for Businesses

1

Know your Gaps

Contact us to assess your current security and privacy operations.

2

Fill the gaps

Based on your gaps, either develop the resources internally or outsource to a competent vendor.

3

Periodically assess

Security is a continuous process and you should be both proactive and reactive.

Lead Researcher's Feedback on the Executive Summary

It's interesting that the data shows that IT businesses do not perform much better at basic cyber security than businesses who are not in the IT industry. With **93,273** compromised accounts across **216 domains,** while 81% don't set expected security headers. It shows there is a gap in their internal security operations.

Train users

Educate users to stop using their business email to sign up for personal services online.

Assess vendors

It's important to assess IT vendors because they might increase your risk exposure.

Compromised credentials

If their credentials are compromised while having access to your network, that's trouble for your org.

HTTPS

A high number of IT business websites (63%) have implemented HTTPS. The pros should lead by example.

Lead Researcher's Feedback on the Executive Summary (Cont'd)

At the national level there is more talk than action in the quantity of countries in the Caribbean that have implemented the expected protections for their citizens and national infrastructure.

Plans/Strategies

Most governments in the Caribbean have not announced a plan to address Cyber Security.

Cyber Crime

Almost 1/3 have a cyber crime plan but at the rate of Cyber Crime, countries could be crippled.

CSIRT

Cyber attacks are inevitable, it's widely discussed. At only 13% implementation, there's a lot of room to improve.

Data Protection Law

Regulations like GDPR force many businesses start to seriously care about protecting people's data & their systems.

We must rethink how we measure “good” Cyber Security.

In 2017, Jamaica was recognized as number one in the Caribbean for Cyber Security based on a survey that measured high-level commitment.

Based on our 2020 data, which measures both high and low-level evidence, Jamaica performed poorly in implementing basic Cyber Security on their websites at either the national level or locally across businesses.

Let’s do more than implement policies and laws without actual cyber security controls.

Work with internationally experienced pros.

Please book a meeting online for your organisation.

g5cybersecurity.com/meeting

1. The **Compromised Accounts** section starts here.

2. The target is 0%, no compromised accounts.

3. Compromised accounts lead to data loss.

4. Contact us HERE to check your accounts for compromises.

Background information on Compromised Accounts

What is this?

These are a mixture of usernames, email addresses and passwords, linked to a domain we analysed, which have been leaked online, usually on the dark web, due to a data breach.

Why is this important?

It is a widely discussed fact that people often reuse the same password across multiple services. When breaches happen, attackers try to sell the data or gain access to user's accounts.

How to protect against?

Everyone needs to be educated and practicing good security habits online such as using unique and strong passwords for each service and implementing good data security controls.

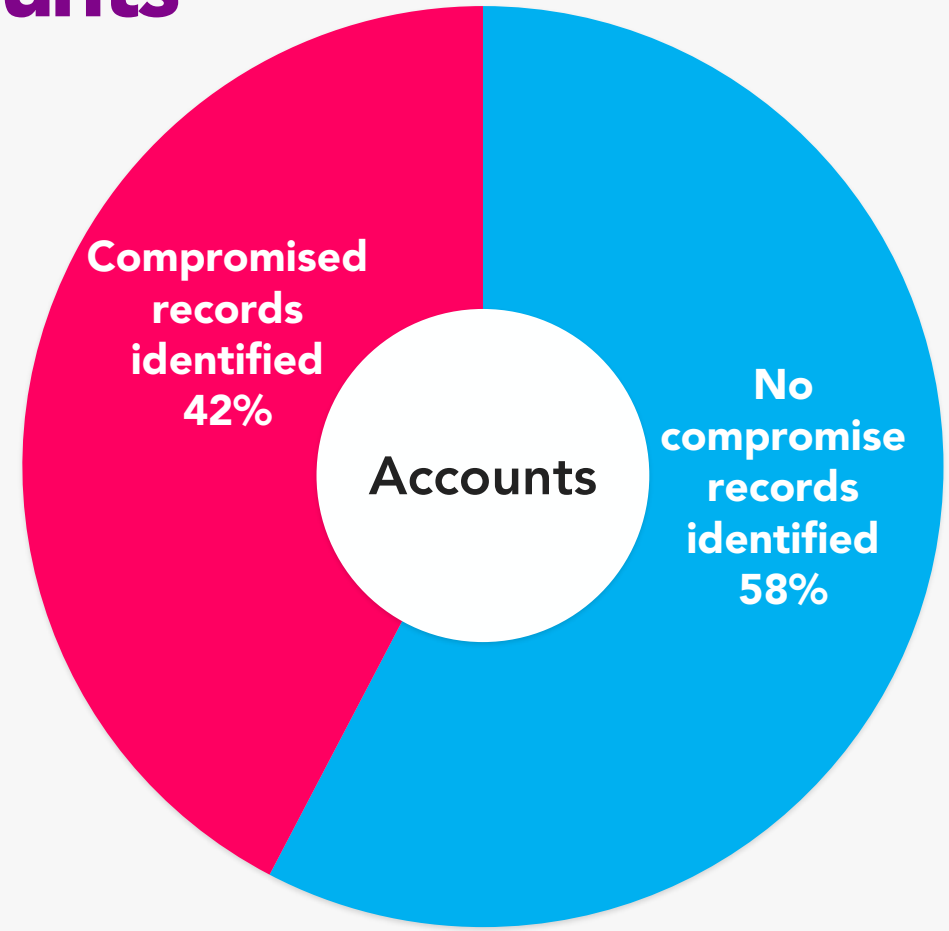
Compromised Accounts Chart

- Domains identified with compromised accounts.

  5,838 records

- Domains without any compromised accounts identified.

  7,953 records



We are partners of SpyCloud

We've partnered with SpyCloud to provide business in the Caribbean and internationally with protection against account takeover and fraud. Through SpyCloud, we identify credentials exposed on the Dark Web and help our clients take real time action.

Contact us to check your organization's exposure.

You can learn more about SpyCloud by visiting spycloud.com.

Compromised Accounts
Quantity and timeline

10, 786, 803

Account credentials are exposed in data breaches belonging to businesses and people operating in the Caribbean.

1 week (Sept 20, 2020)

ago was the time between the newest discovered compromised account and when we released this report.

Compromised Accounts profile of the top 10 affected businesses

1. International Audit firm
1,105,451 records.
2. International Audit firm
1,077,139 records.
3. International Audit firm
903,149 records.
4. International Hotel chain
523,160 records.
5. International Hotel chain
484,477 records.
6. International Logistics
467,427 records.
7. International Audit firm
467,169 records.
8. International Logistics
429,287 records.
9. International Logistics
423,756 records.
10. International Pharmaceutical company 382,154 records.

Yes! You can contact us to assess your organization's domains and email addresses for exposure on the dark web.

We can also protect your business with a real time solution that integrates with Active Directory to detect and protect compromised credentials from being taken takeover by attackers.

Contact Us

Compromised Accounts (Highest to Lowest)

№	Country	The target is 0%. No credentials exposed on the Dark Web.
1	Puerto Rico	23.0% (1344)
2	Jamaica	16.4% (957)
3	Cayman Islands	7.6% (445)
4	Barbados	6.5% (381)
5	Bermuda	5.6% (328)
6	Aruba	4.7% (276)
7	Belize	4.7% (239)
8	Dominican Republic	3.1% (182)
9	Curaçao	2.9% (168)
10	Grenada	2.3% (133)

Compromised Accounts (Highest to Lowest)

№	Country	The target is 0%. No credentials exposed on the Dark Web.
11	Cuba	2.0% (119)
12	St. Lucia	1.9% (110)
13	Turks and Caicos Islands	1.7% (102)
14	British Virgin Islands	1.7% (100)
15	US Virgin Islands	1.7% (100)
16	Bahamas	1.4% (84)
17	Guyana	1.4% (79)
18	Guadeloupe	1.3% (76)
19	St. Kitts and Nevis	1.2% (70)
20	Suriname	1.2% (69)

Compromised Accounts (Highest to Lowest)

№	Country	The target is 0%. No credentials exposed on the Dark Web.
21	Haiti	1.1% (66)
22	St. Maarten	1.0% (57)
23	Trinidad and Tobago	1.0% (57)
24	Anguilla	0.9% (55)
25	Dominica	0.9% (55)
26	St. Vincent and the Grenadines	0.8% (46)
27	Antigua and Barbuda	0.7% (41)
28	St. Martin	0.5% (27)
29	Bonaire, St. Eustatius and Saba	0.4% (21)
30	Martinique	0.3% (18)

Compromised Accounts (Highest to Lowest)

№	Country	The target is 0%. No credentials exposed on the Dark Web.
31	St. Barthélemy	0.3% (20)
32	Montserrat	0.2% (13)

Lead Researcher's Feedback on Compromised Accounts (cont'd)

The 4th and 5th largest countries in the Caribbean took the number 1 and 2 spots in the highest numbers of compromised credentials. In 2017, **Jamaica** was recognized by the ITU Global Cybersecurity Agenda (GCA) as number **one** in the Caribbean for Cyber. However with Jamaica having the second highest quantity of compromised credentials on the Dark Web, it's clear that how we measure Cyber Security must evolve.

Below are two references from Jamaica's largest media companies reporting on this ranking. Reference:

- http://www.jamaicaobserver.com/news/jamaica-ranks-number-one-for-cybersecurity-in-caribbean_105305
- http://jamaica-gleaner.com/article/news/20170719/jamaica-ranks-number-one-cyber-security-region

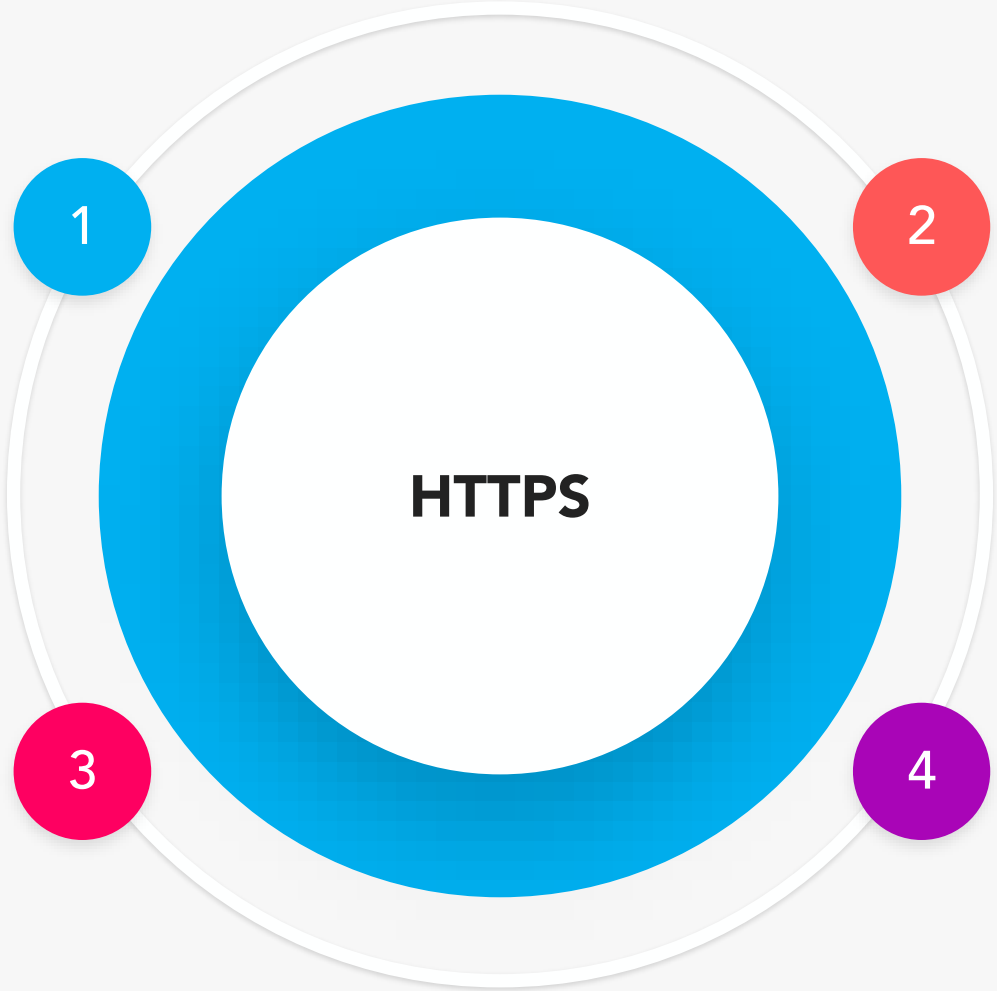
PS: As at Oct 1, 2020 none of the two websites above use HTTPS. ☺

Hi, I'm Gavin Dennis!

Are you sceptical about whether the data is genuine?

Then join one of our fortnightly Data Chat online and select a sample of the data yourself.

Click here to register



1. The **HTTPS** section starts here.

2. The target goal is 100%.

3. HTTPS protects web communications.

4. Contact us HERE to protect your website from cyber attacks.

Background Information on HTTPS

What is this?

HTTPS is a secure way to send data between a web server and a web browser. It is the secure version of the HTTP protocol, which powers the web.

Why is it important?

1. HTTPS protects the integrity of websites.
2. HTTPS protects the privacy and security of users.
3. HTTPS is the future of the web.

How to implement?

Good HTTPS can be implemented by installing a valid SSL certificate on a web server. Certificates can be obtained for free or at a small cost, depending on a few factors.

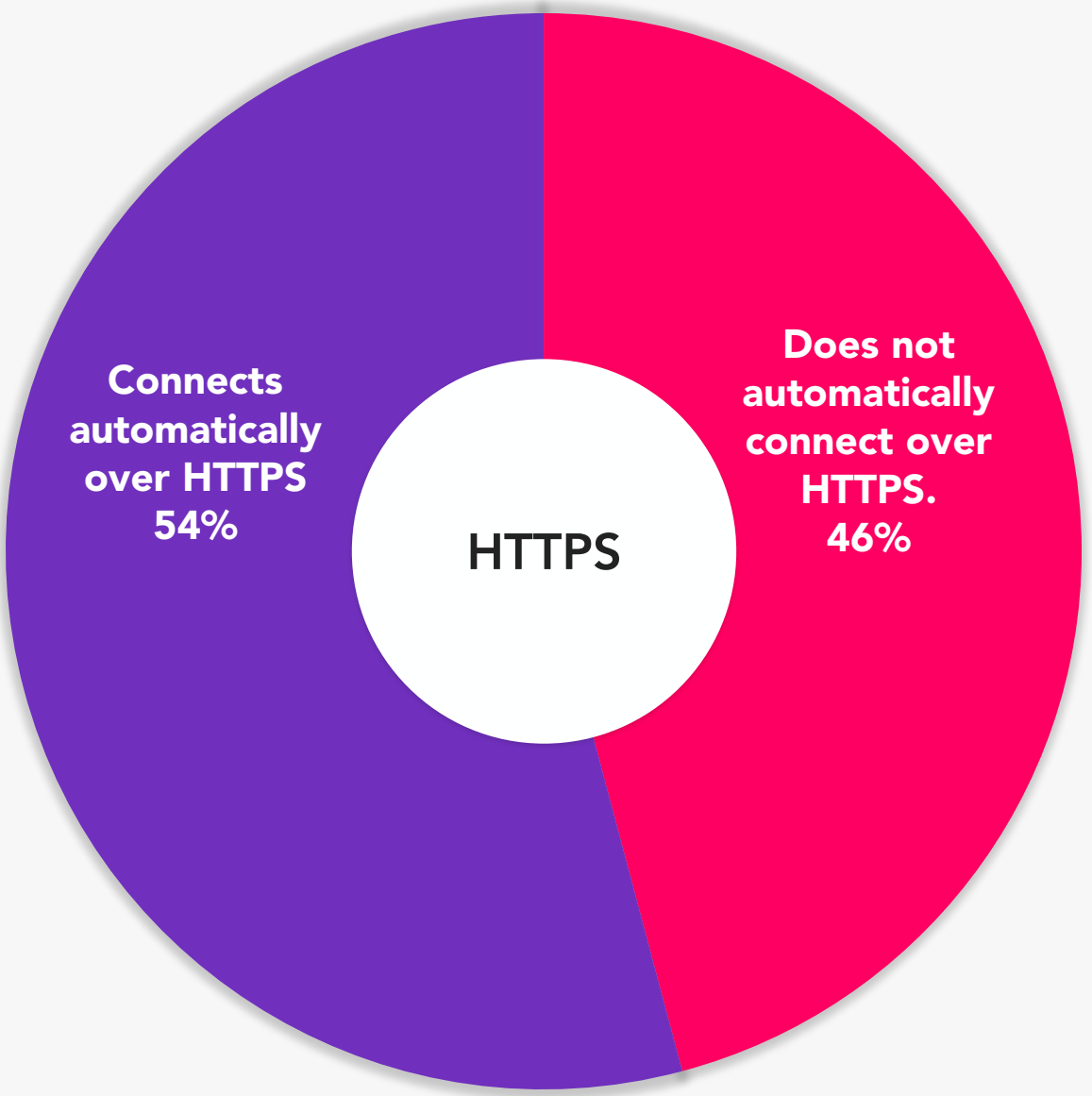
HTTPS Usage

- Automatically connects over HTTPS.

  7,468

- Does not automatically connect over HTTPS.

  6,324



HTTPS
How to interpret the bars coming up

Break down

0-100%

The following figures are as a percentage of the **7,468** websites that **do** automatically connect over HTTPS when visited by a user.

HTTPS Usage (Highest to Lowest) – by percentage

№	Country	This shows the distribution of the 7,468 websites that use HTTPS.
1	Jamaica	15.8% (1,179)
2	Puerto Rico	13.9% (1,035)
3	Cayman Islands	7.9% (593)
4	Barbados	7.5% (558)
5	Aruba	5.9% (441)
6	Dominican Republic	5.5% (413)
7	Belize	4.9% (365)
8	Bermuda	4.2% (313)
9	Grenada	3.1% (235)
10	Curacao	3.1% (232)

HTTPS Usage (Highest to Lowest) – by percentage

№	Country	This shows the distribution of the 7,468 websites that use HTTPS.
11	Cuba	2.6% (192)
12	Turks and Caicos Islands	2.1% (159)
13	St. Lucia	2.1% (155)
14	Martinique	2.0% (150)
15	Guyana	2.0% (146)
16	St. Kitts and Nevis	1.7% (124)
17	US Virgin Islands	1.6% (121)
18	Bahamas	1.6% (120)
19	British Virgin Islands	1.4% (107)
20	Anguilla	1.3% (99)

HTTPS Usage (Highest to Lowest) – by percentage

№	Country	This shows the distribution of the 7,468 websites that use HTTPS.
21	Guadeloupe	1.3% (95)
22	Trinidad and Tobago	1.2% (93)
23	Haiti	1.2% (91)
24	St. Maarten	1.2% (88)
25	Suriname	1.1% (80)
26	Dominica	0.9% (70)
27	Antigua and Barbuda	0.7% (54)
28	St. Vincent and the Grenadines	0.7% (50)
29	St. Martin	0.5% (38)
30	Bonaire, St. Eustatius and Saba	0.5% (37)

HTTPS Usage (Highest to Lowest) – by percentage

№	Country	This shows the distribution of the 7,468 websites that use HTTPS.
31	St. Barthélemy	0.3% (22)
32	Montserrat	0.2% (13)

Lead Researcher's Fedback on Security Headers

HTTPS is a good indicator that a business or website operator has started to care about security. A website is what the world sees. As such, if a website does not use HTTPS, it is usually a strong indicator of what is happening internally, which the world cannot see.

Do more than HTTPS

Compromised credentials are being stolen from multiple sources vectors.

Admins need to care

Website administrators need to protect their login details by using HTTPS.

Stop using TLS 1.0 and 1.1

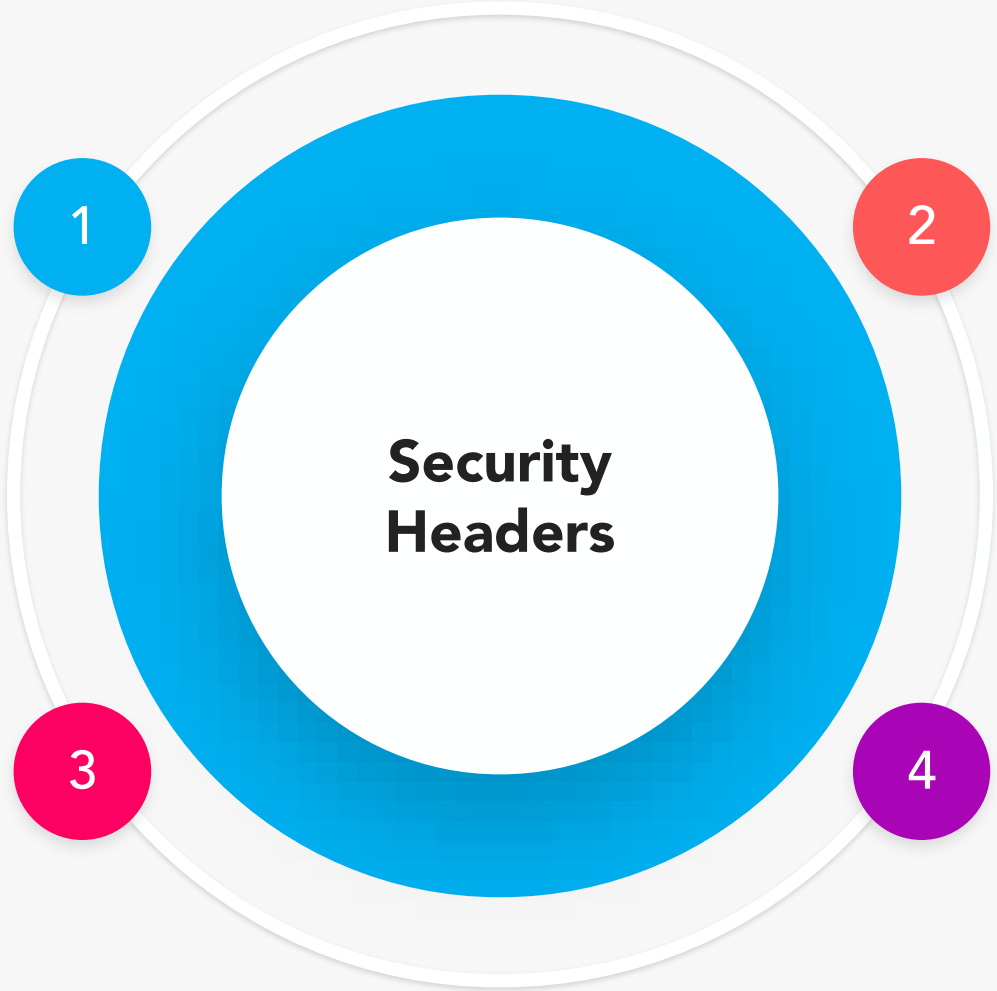
We identified high usage of weak protocols but will release this next year.

HTTPS helps your ranking

Websites that use HTTPS is being ranked higher by Search Engines.

Learn more about HTTPS

help.g5cybersecurity.com	https://help.g5cybersecurity.com/hc/en-gb/articles/360006996558-How-to-implement-HTTPS-for-websites-and-web-applications
Cloudflare.com	https://www.cloudflare.com/learning/ssl/what-is-https/
Web.dev	https://web.dev/why-https-matters/



1. The **Security Headers** section starts here.

2. The target goal is 100%.

3. Security Headers helps to protect websites and users.

4. Contact us HERE to protect your website from cyber attacks.

Background information on Security Headers

What is this?

Security Headers are web server response headers that can restrict modern browsers from running into common vulnerabilities. They protect both the web server and users.

Why is this important?

If Security Headers are not set, then both the users and the web server are left unnecessarily vulnerable to attacks such as Cross-Site Scripting (XSS), Session Hijacking and Click-jacking.

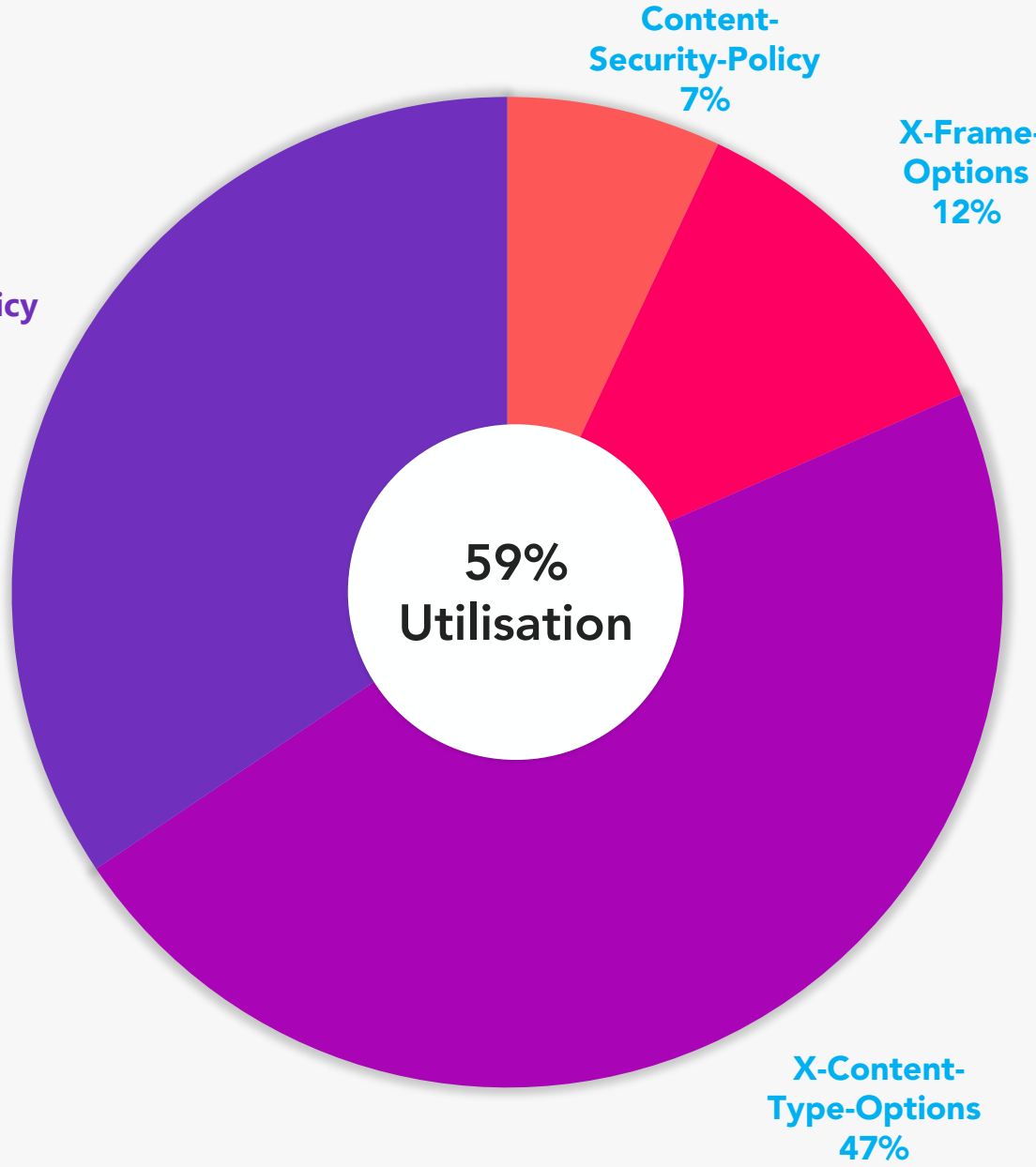
How to implement?

Security Headers can be set by modifying a web server's configuration file such as **.htaccess** (Linux), **httpd.conf** (Linux) or **web.config** (IIS on Windows).

Security Headers Usage

A total of **68,955** headers were expected, which is 5 headers for each of the **13,791** websites analysed.

28,358 headers were missing, which represents a 41% of **68,955**. **40,597** headers are being used which represents a 59% utilization of **68,955** expected headers.

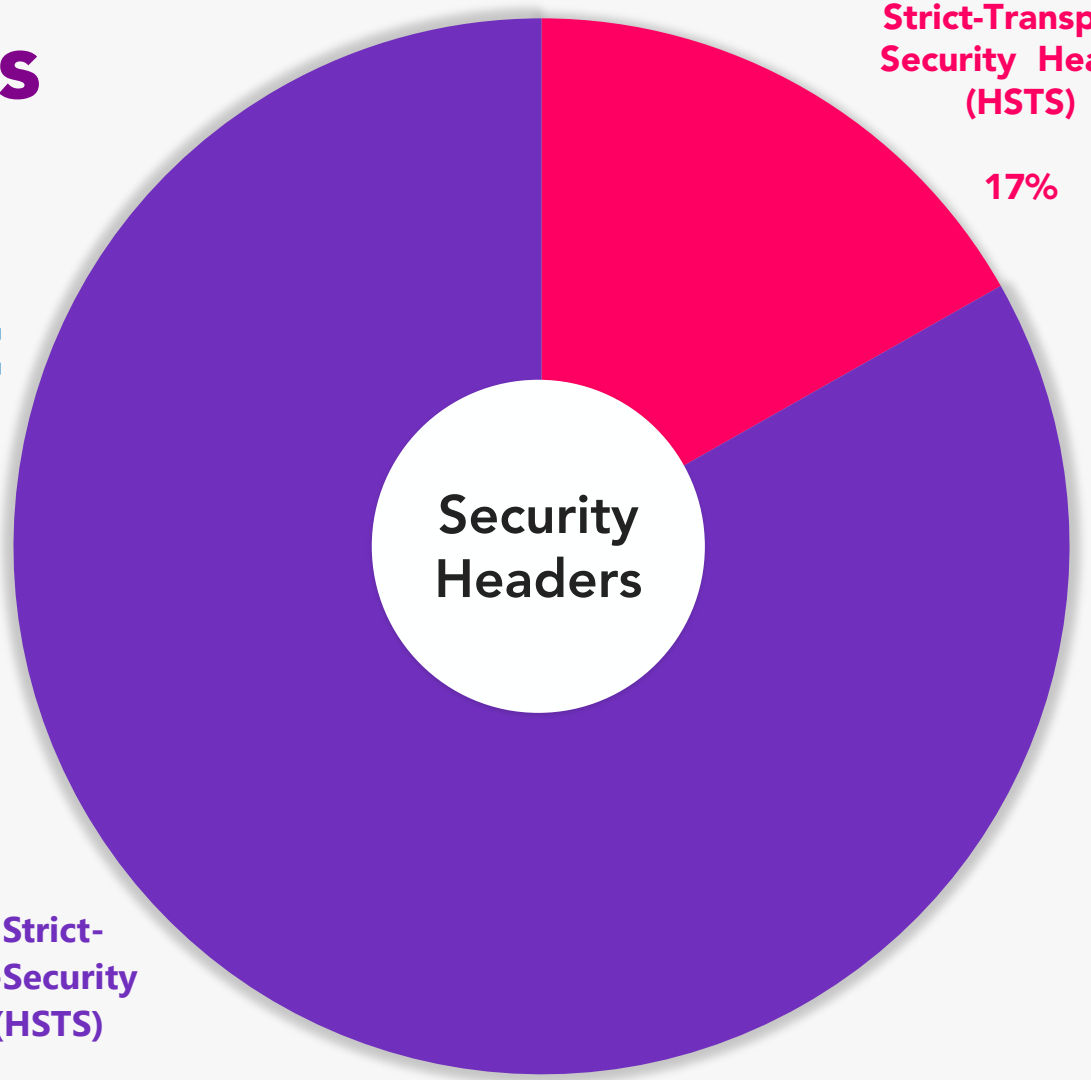


Security Headers Usage

Strict-Transport Security

This header analysis is only applicable to the **7,468** websites that do connect over HTTPS.

So 83% of 7,468 (ie. 6,214 HTTPS websites) set this header.



Security Headers Configuration

Strict-Transport-Security (HSTS) Header

Enforces connections over HTTPS only for websites that use HTTPS. It protects against downgrade attacks and cookie hijacking.

Content-Security-Policy Header

Controls the way browsers render and load content on pages. CSP protects against several attacks, including cross-site scripting.

X-Frame-Options Header

Protects against Click-jacking. The CSP frame-ancestors directive from **Content-Security-Policy** can be used instead of setting this header.

Security Headers Configuration

Feature-Policy Header

Allows website owners to toggle on or off certain features of web browser and APIs. E.g. access to camera and microphone.

X-Content-Type-Options Header

Prevents browsers from interpreting files as a different MIME type than what is specified in the Content-Type header.

Disclose version numbers in headers

Default response headers were identified that disclose software versions.

Security Headers Configuration – Issues (Based on 7,468 HTTPS websites)

0.7%

Sets inactive HSTS

This means the HSTS response header is set but has an age set to "0", which disables the purpose of the header.

0.1 %

Set multiple HSTS

The HSTS response header was seen multiple times in a single response. This indicates a misconfiguration.

0.1 %

Set multiple X-Frame-Options

The **X-Frame-Options** header was seen multiple times in a single response. This indicates a misconfiguration.

Lead Researcher's Feedback on Security Headers

Setting Security Headers can sometimes be tedious, and if not done properly can disable some user functionality on a website or web application.

From my experience, many website administrators either don't know that security headers should be implemented or see them as insignificant.

Minimal Misconfigurations

For the headers set, errors detected were below 1%.

Easily detectable

You can visit https://securityheaders.com and enter a domain to see missing headers.

Protect users

If security awareness is effective, customers will start to publicly call out insecure websites.

Accountability

Businesses need to hold their website administrators accountable for security.

Learn more about Security Headers

help.g5cybersecurity.com	https://help.g5cybersecurity.com/hc/en-gb/sections/360002066757-Web-Security
OWASP	https://owasp.org/www-project-secure-headers/
Keycdn.com	https://www.keycdn.com/blog/http-security-headers

Hi, I'm Gavin Dennis!

Let's talk about the data together.

Then join our fortnightly Data Chat.

Click here to register

National Cyber Security Plans/ Strategies

1. The **National Cyber Security Plan** section starts here.
2. Every country should have a Cyber Security Plan.
3. This plan helps governments to operate securely.
4. Contact us HERE with your questions and feedback.

Background information on National Cyber Security Plan/Strategies

What is this?

The **plan** is an intended set of actions about **what** will be done, while the **strategy** outlines how to improve the security and resilience of national infrastructures and services.

Why is this important?

A documented plan/strategy helps to provide a structure towards achieving the goal or objectives of protecting a nation against cyber attacks.

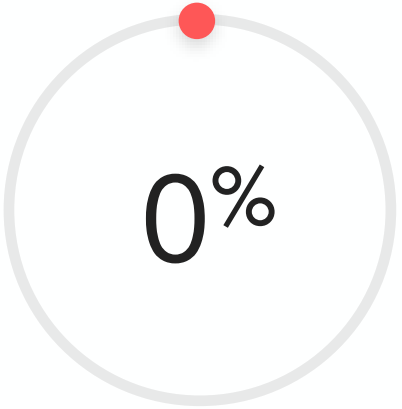
How to implement?

A country's government lead the action with competent cyber professionals to define the country's requirements, draft and approve a plan or strategy.

Dashboard
National Cyber Security Plans/Strategies

of countries have a documented National Cyber Security Plan

- Positive but poor



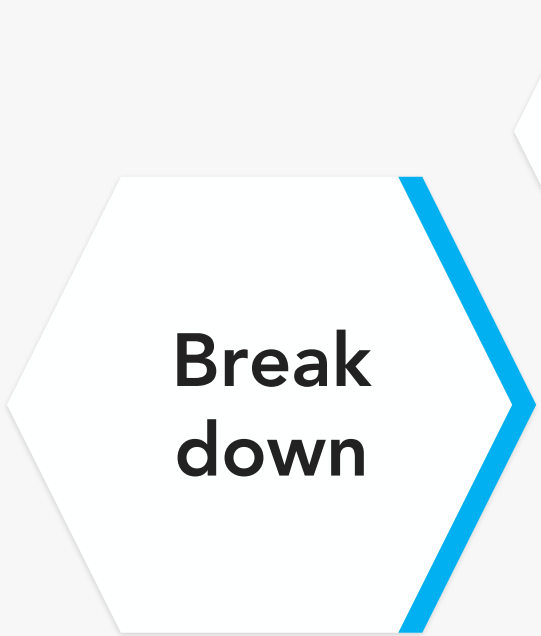
of the remaining countries have announced a draft.

- Poor

of countries are without a National Cyber Security Plan

- Poor

National Cyber Security Plans/Strategies
How to interpret the bars coming up



0% The document has not been publicly announced by the government as drafted.

50% The document has been publicly announced by the government as drafted.

100% The document is officially finalized by the government.

National Cyber Security Plans/Strategies per Country/ Territory (Highest to Lowest)

№	Country	Progress
1	Bermuda	100%
2	Dominican Republic	100%
3	Jamaica	100%
4	Trinidad and Tobago	100%
5	Belize	50%
6	Remaining Countries	0% (27 countries)

List of National Cyber Security Plans/Strategies

Country	Document name (Click the doc title to visit the reference)
Bermuda	Bermuda Cybersecurity Strategy 2018 - 2022
Dominican Republic	National Cybersecurity Strategy 2018-2021
Jamaica	National Cyber Security Strategy
Trinidad and Tobago	National Cyber Security Strategy
Belize	National Cybersecurity Strategy - Towards A Secure Cyberspace 2020-2023

Lead Researcher's Feedback on National Cyber Security Plans/ Strategies

Without a documented plan/strategy, it increases the difficultly for everyone across government, private sector and citizens to have a common and clear understanding of what needs to be done.

More countries are without a cyber security plan than a Cyber Crime Law.

Plans should define "what should be done"

Strategies should define "How it should be done"

Some drafts exist

It's good that 3 countries have drafts, but it's time to move them to being finalized.

Plans need action

A document by itself does nothing, we must execute on these idealistic plans.

1. The **National Cyber Crime Law** section starts here.
2. Every country should have a Cyber Crime Law.
3. This law punishes people who commit cyber crimes.
4. Contact us HERE with your questions and feedback.

Background information on Cyber Crime Laws

What is this?

A Cyber Crime Law prohibits harmful offences committed via the internet or using various forms of computer technology.

Why is this important?

The world relies heavily on technology for survival and some people may try to use technology to cause harm to others and must be punished. The law aims to deter and remedy any harm.

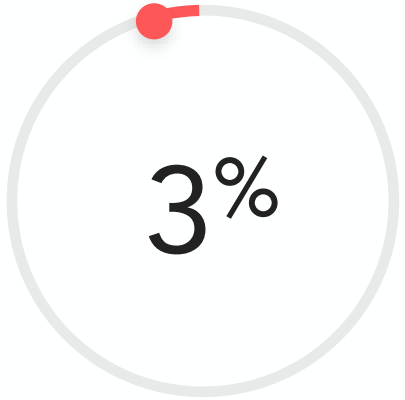
How to implement?

A country's government leads the action with cyber professionals and others to create a law that outlines what activities are cyber crimes and the consequences for those who commit them.

Dashboard
Cyber Crime Laws

of countries have a Cyber Crime Law.

- Positive but poor



of the remaining countries have announced a draft.

- Poor

of countries are without a National Cyber Security Plan.

- Poor

Cyber Crime Laws
How to interpret the bars coming up

0% The document has not been publicly announced by the government as drafted.

50% The document has been publicly announced by the government as drafted.

100% The document is officially finalized by the government.

Cyber Crime Law per Country/ Territory (Highest to Lowest)

№	Country	Progress
1	Antigua and Barbuda	100%
2	Bahamas	100%
3	Barbados	100%
4	Bermuda	100%
5	British Virgin Islands	100%
6	Dominica	100%
7	Grenada	100%
8	Guyana	100%
9	Jamaica	100%
10	St. Kitts and Nevis	100%

Cyber Crime Law per Country/ Territory (Highest to Lowest)

№	Country	Progress
11	St. Lucia	100%
12	Trinidad and Tobago	100%
13	St. Vincent and the Grenadines	50%
14	Remaining Countries	0% (19 countries)

List of Cyber Crime Laws

Country	Document name (Click the doc title to visit the reference)
Antigua and Barbuda	Electronic Crimes Act, 2018
Bahamas	The Computer Misuse Act (Cma), 2003
Barbados	Computer Misuse Act, 2005
Bermuda	Computer Misuse Act, 1996
British Virgin Islands	Computer Misuse And Cybercrime Act, 2019

List of Cyber Crime Laws

Country	Document name (Click the doc title to visit the reference)
Dominica	Computer And Computer Related Crimes Act Of 2005
Grenada	Electronic Crimes Act, 2013
Guyana	Cyber Crime Act, 2018
Jamaica	Cybercrimes Act, 2015
St. Kitts and Nevis	Electronic Crimes Act, 2009

List of Cyber Crime Laws

Country	Document name (Click the doc title to visit the reference)
St. Lucia	Computer Misuse Act, Cap 8.14 (No link available)
Trinidad and Tobago	The Computer Misuse Act, 2000
St. Vincent and the Grenadines	St Vincent and The Grenadines Cybercrime Bill 2016

Lead Researcher's Feedback on Cyber Crime Laws

There have been numerous cyber attacks and data breaches across the Caribbean but there are minimal reports online of people being prosecuted for Cyber crimes.

This opens the question: Do these nations have the capabilities to catch cyber criminals?

Progressive

With 12 or 32 countries having a law, it should give motivation to the others.

Improve access

Governments need to make the legal document available on their website, 50% are on other sites.

Large but slow

Strangely, large countries do not have such laws (Puerto Rico, Haiti and The Dominican Republic).

Law needs resources

It's good to have the laws but competent professionals need to be developed to do the work.

Hi there!

Let’s talk about the data together.

Please join our fortnightly Data Chat.

Click here to register

National Cyber Incident Response Team

1. The **National Cyber Incident Response Team** section starts here.
2. Every country should have a National Cyber Incident Response Team.
3. This team responds to cyber attacks and breaches.
4. Contact us HERE with your questions and feedback.

Background information on National Cyber Incident Response Team

What is this?

National Cyber Incident Response Team is responsible for responding to security breaches, viruses and other potentially catastrophic incidents facing a country.

Why is this important?

Every country using technology is at risk to cyber attacks which can cripple their economy. When attacks happen there needs to be a team to deal with them.

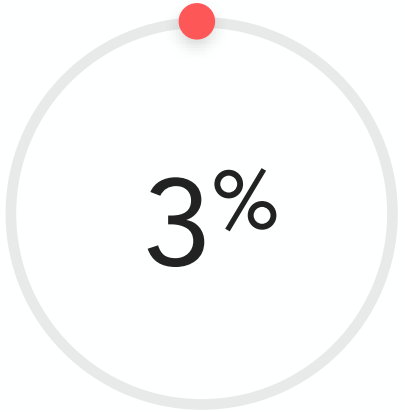
How to implement?

A country's government lead the action to create a competent team to respond to cyber attacks and go through the Incident Response (IR) process.

Dashboard
National Cyber Incident Response Teams

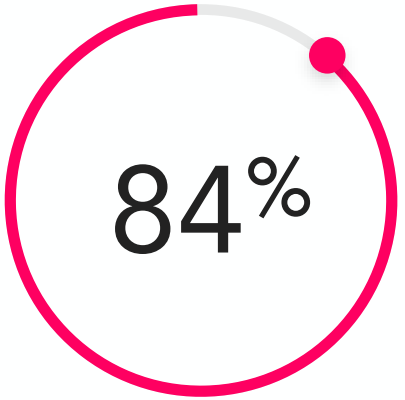
of countries have a National Cyber Incident Response Team

- Positive but poor



of the remaining countries have announced they will start a team

- Poor



of countries are without a National Cyber Incident Response Team

- Poor

National Cyber Incident Response Team
How to interpret the bars coming up

0% The government has not announced plans to form a National Cyber Incident Response Team.

50% The government has announced that it has started to form a National Cyber Incident Response Team.

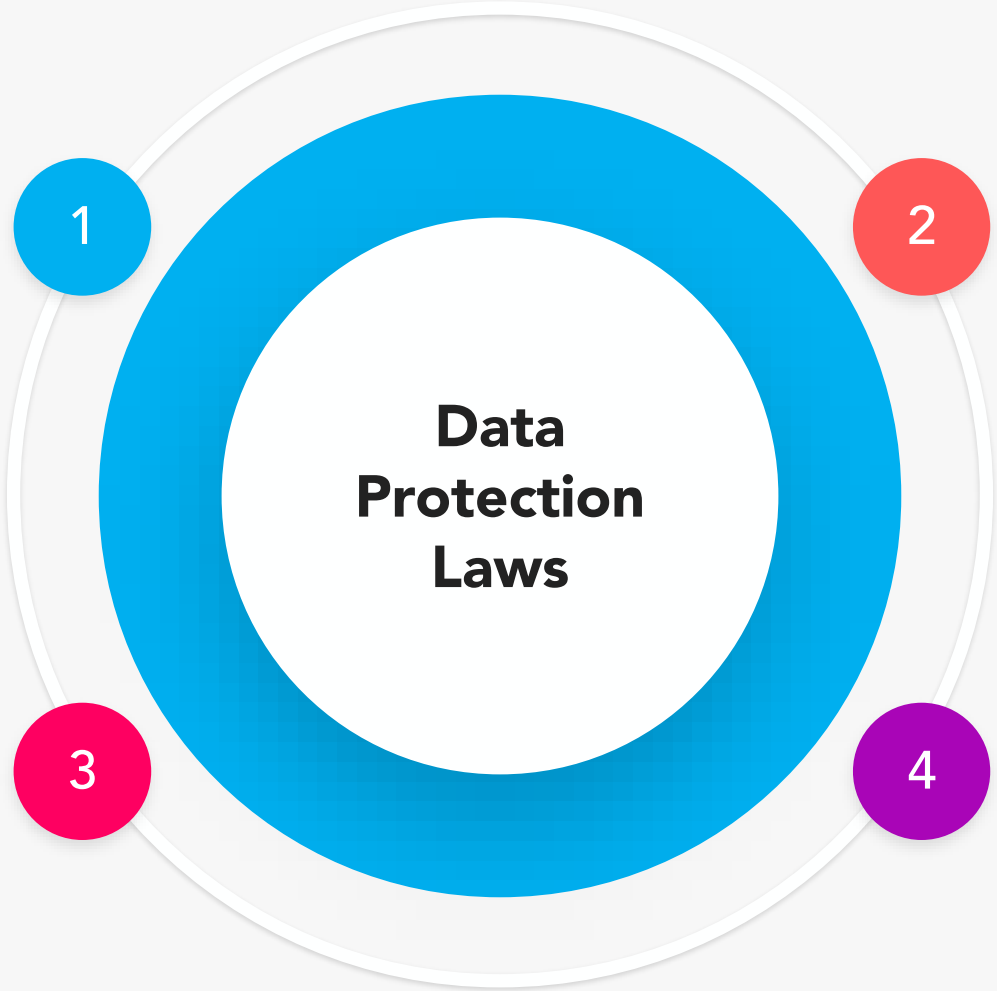
100% The government has completed forming a National Cyber Incident Response Team.

National Cyber Incident Response Team per Country/ Territory (Highest to Lowest)

№	Country	Progress
1	Barbados	100%
2	Guyana	100%
3	Jamaica	100%
4	Trinidad and Tobago	100%
5	Dominican Republic	50%

National Cyber Security Plans
Document list

Country	Team name
Barbados	NCIRT (National Computer Incident Response Team)
Guyana	Guyana National Computer Incident Response Team
Jamaica	Jamaica Cyber Incident Response Team (JaCIRT)
Trinidad and Tobago	Trinidad and Tobago Cyber Security Incident Response Team (TTCSIRT)
Dominican Republic	Cyber Incident Response Team



1. The **Data Protection Laws** section starts here.

2. Every country should have a Data Protection Law.

3. This law helps to protect people's personal data.

4. Contact us HERE to assess your orgs Data Protection Compliance.

Background information on Data Protection Laws

What is this?

A Data Protection Law controls how personal information can be used and your rights to ask for information about yourself.

Why is this important?

Because the world is becoming so digitized, people need to share their personal data for needed purposes, but that data also needs to be appropriately protected.

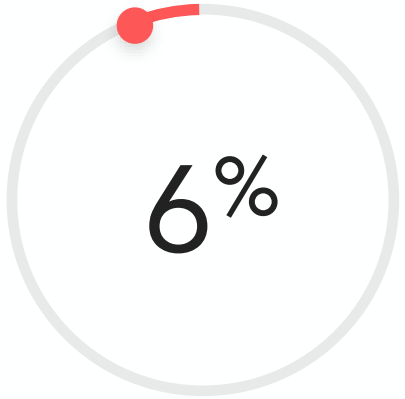
How to implement?

A country's government leads the action with data protection professionals and others to create a law outlining how its citizens data must be treated and the consequences if those requirements are broken.

Dashboard
Data Protection Laws

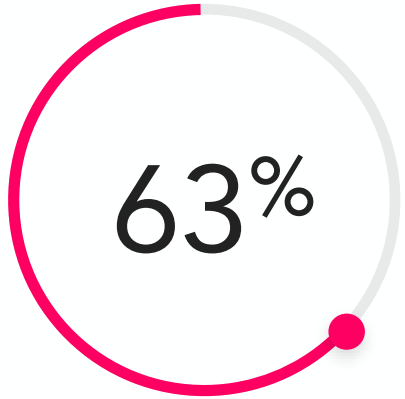
of countries have a Data Protection Law.

- Positive but poor



of the remaining countries have announced a draft.

- Poor



of countries are without a National Cyber Security Plan.

- Poor

Data Protection Laws
How to interpret the bars coming up

0% The document has not been publicly announced by the government as drafted.

50% The document has been publicly announced by the government as drafted.

100% The document is officially finalized by the government.

Data Protection Laws per Country/ Territory (Highest to Lowest)

№	Country	Progress
1	Antigua and Barbuda	100%
2	Bahamas	100%
3	Barbados	100%
4	Bermuda	100%
5	Cayman Islands	100%
6	Curacao	100%
7	Dominican Republic	100%
8	St. Kitts and Nevis	100%
9	St. Lucia	100%
10	St. Vincent and the Grenadines	100%

Data Protection Laws per Country/ Territory (Highest to Lowest)

№	Country	Progress
11	Trinidad and Tobago	100%
12	Jamaica	50%
13	Suriname	50%
	Remaining Countries	0% (20 countries)

List of Data Protection Laws

Country	Document name (Click the doc title to visit the reference)
Antigua and Barbuda	Data Protection Act 2013
Bahamas	Data Protection (Privacy of personal information), 2003
Barbados	Data Protection Act, 2019
Bermuda	Personal Information Protection Act, 2016
Cayman Islands	The Data Protection Law, 2017

List of Data Protection Laws

Country	Document name (Click the doc title to visit the reference)
Curacao	The Personal Data Protection Act, 2013 (No document link available)
Dominican Republic	Protection of Personal Data, 2013
St. Kitts and Nevis	Data Protection Act, 2018 (No document link available)
St. Lucia	Data Protection Act, 2011
St. Vincent and the Grenadines	Privacy Act, 2003

List of Data Protection Laws

Country	Document name (Click the doc title to visit the reference)
Trinidad and Tobago	Data Protection Act, 2011
Jamaica	Data Protection Act, 2020
Suriname	Data Protection Bill, 2018

Lead Researcher's Feedback on Data Protection Laws

The GDPR has had such a significant impact on the world that many countries are rushing to implement similar laws/regulations.

From experience, such regulations force businesses to respect people's data. **Facebook's** bad history before GDPR is a prime example.

New adoption

A very similar implementation rate was noticed for Data Protection vs Cyber Crime Laws.

International Influence

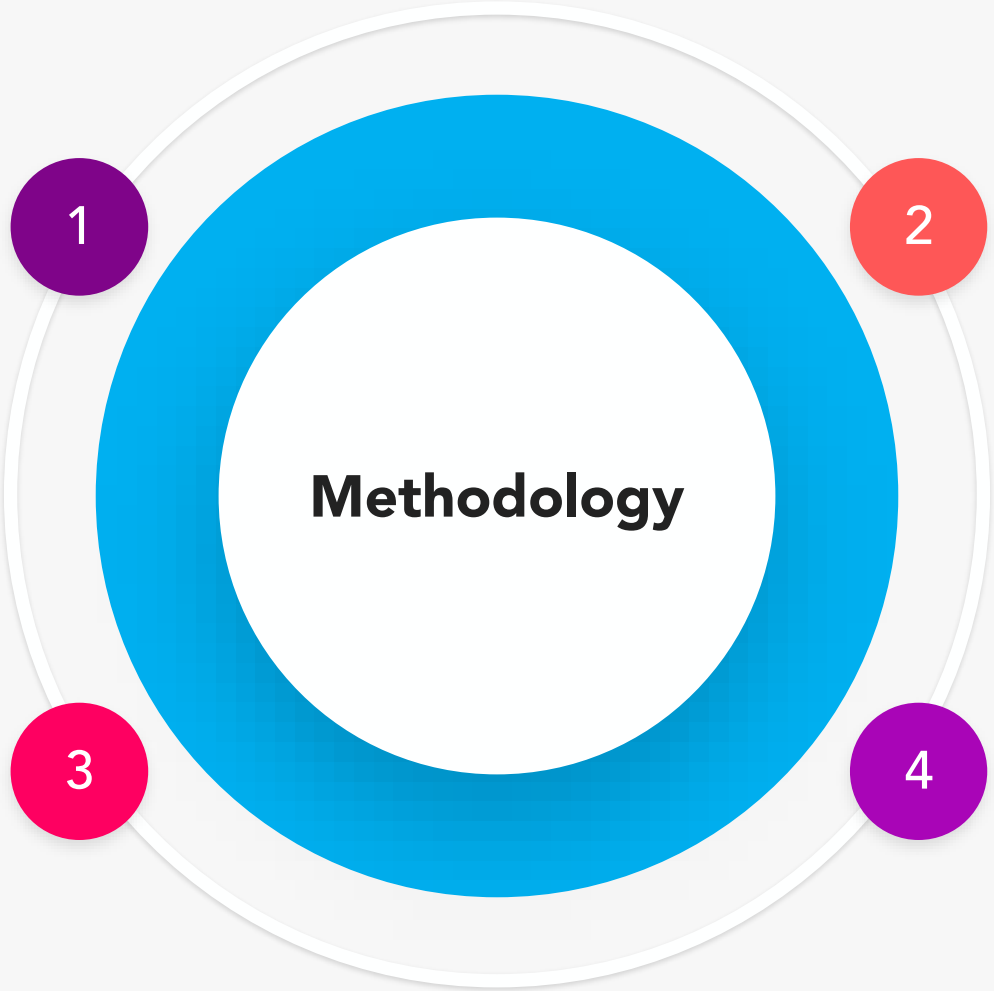
Regulations like the GDPR are motivating other countries to create their own.

Small and quick

The smallest set of islands have been the earliest adopters. Kudos to them.

Laws force business to care

From experience, people's data is abused less due to laws and regulations.



1 The **Methodology** section starts here.

2 This section outlines how we approached the overall analysis.

3 Understanding our approach helps you to use the data.

4 Contact us HERE with your questions and feedback.

Methodology for Selecting Domains

Only some types of Top-Level Domains (TLDs) were considered as valid.

You can learn more about the different types of TLDs at https://www.cisecurity.org/spotlight/cybersecurity-spotlight-top-level-domains-tld/

Any website that uses a temporary domain was excluded.

Included TLDs

- generic top-level domains (gTLD)
- country code top-level domains (ccTLD)
- sponsored top-level domains (sTLD)
- restricted generic top-level domains (grTLD)

Excluded TLDs

- infrastructure top-level domain (ARPA)
- test top-level domains (tTLD)
- Temporary domains (e.g. *.wix.com)

Methodology for Included TLDs

- .gov.* and its first sub-domains are treated as root domains. E.g. gov.jm and cirt.gov.jm are treated as being on the same level. .gov is an **sTLD** and .jm is a **ccTLD. gov.jm is** accessible but other Caribbean non-sTLDs don't operate this way. E.g. You cannot access **com.jm** as a website.

- Domains on other TLDs are treated normally. Meaning, when a new domain name is created, the root domain and sub-domain are treated as being on a separate level, as you expect.

E.g. **example.com** is the root domain would be included while **test.**example.com is a sub-domain and would be excluded.

Methodology for Selecting Domains

Initially, we shortlisted over 200K domains but when we completed verification, only 12K were valid. This is an example of how thoroughly our team checked to ensure the population of websites was accurate.

What qualifies a website?

Websites must state on either their pages or social media account that they are operated by a business or person in the Caribbean.

Characteristics

A website must provide a local phone number or address in the Caribbean. In minor cases our team had to verify a website through it's social media accounts or other third-parties.

Methodology for Excluding some valid domains

Do you remember that on a previous page, we mentioned that **.gov** domains and their first level sub-domains are treated as being a root domain? Well some of those first level sub-domains are not designed to be accessible as a web page and as such were excluded. Such as:

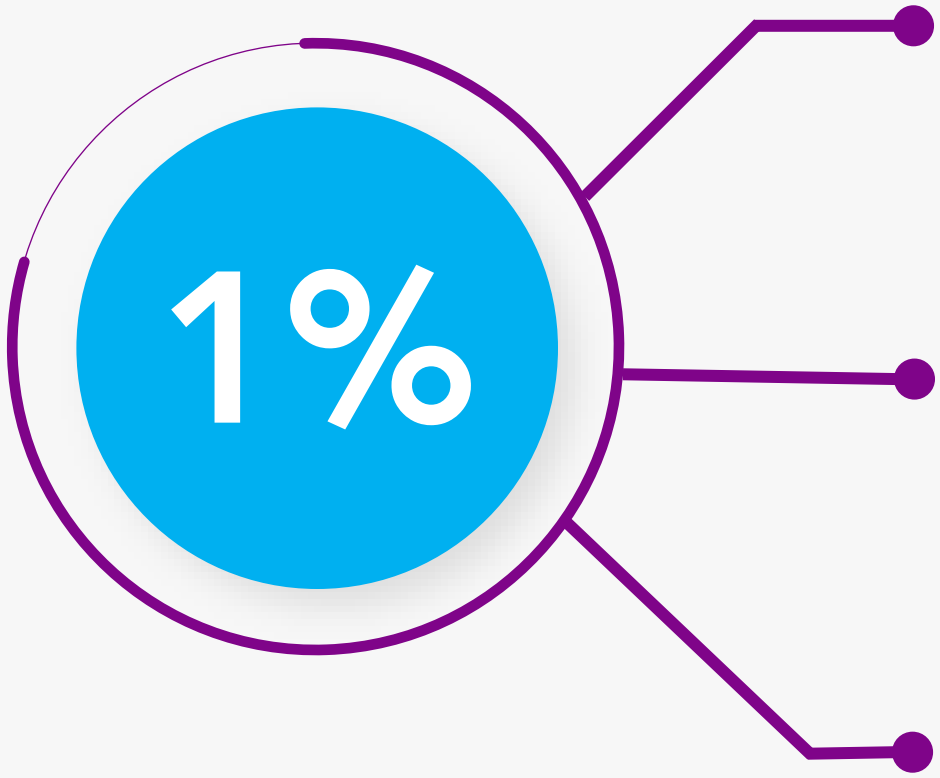
- Email automatic configuration (e.g. autodiscover.gov.*)
- Name servers (e.g ns.gov.*)

Please send your questions to support@g5cybersecurity.com.

Methodology for Classifying Websites by Country/Territory

- If a Caribbean website states it has operations in multiple countries, then the root domain is attributed to the country with its Head Office.
- If no Head Office is stated or can be identified otherwise, then the root domain is attributed to the largest country/territory it operates in within the Caribbean.

Margin of Error



All websites were visited by both a person on our research team and an automated system.

A person checks that each website provides either a phone number or address in the Caribbean.

We keep logs of the checks done to ensure the results are trustworthy.

Limitations on Statistics

The statistics we provide are based on analysis done between September 20-30, 2020.

As such, you should factor in the element of security updates and improvements as time passes.

Websites content get updated often.

People and hosting providers make updates periodically and as such our results website security statistics are as at September 20-30, 2020.

Some websites are abandoned

During analysis we identified 3 websites which became suspended. This is usually the result of outstanding payments to the hosting provider.

Common questions and answers

Why only partial industry statistics?	We are still assessing the risk of providing industry level statistics for all industries and countries. We hope to include it next year.
Why are no company names shown?	This is to protect the privacy and minimize finger-pointing vulnerable companies who might not even be aware they have security gaps.
How were websites identified and analysed?	We used our amazing security skills to identify domains, then we verified whether they belonged to a business or person in the Caribbean.

Common questions and answers

How can these statistics be verified?	We provide a monthly online session where people can select a sample of data and verify.
Are data tables available for analysts?	We are exploring providing a data dump for next year with the company names masked.
What does G5 Cyber Security, Inc. do?	We primarily provide **Cyber Security and Data Privacy** services to help companies protect against cyberattacks and data privacy breaches.

References

1. https://www.cloudflare.com/learning/ssl/what-is-https/

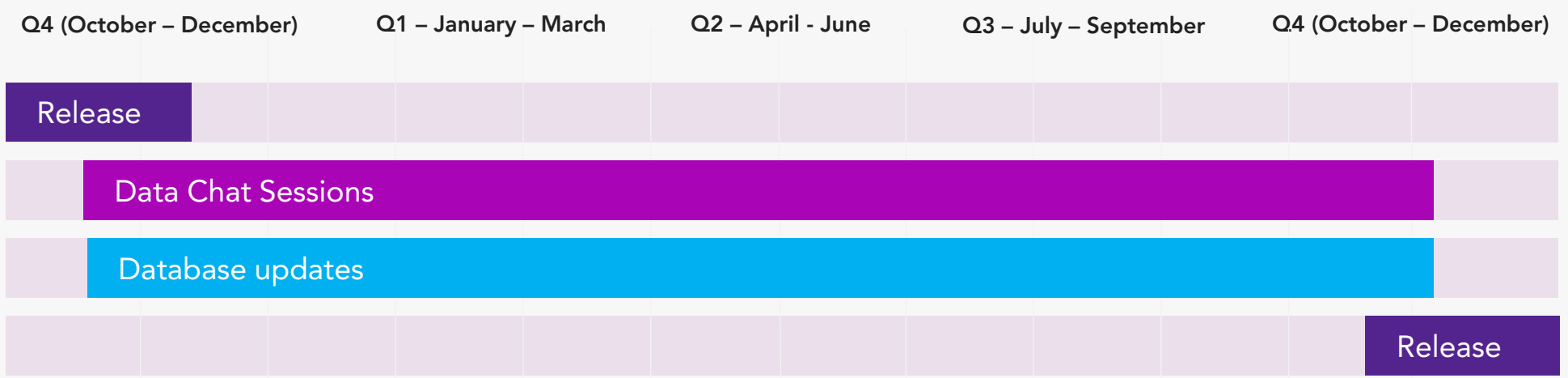
Hi, I'm Gavin Dennis!

Are you sceptical about whether the data is genuine?

Then join one of our fortnightly Data Chat online and select a sample of the data yourself.

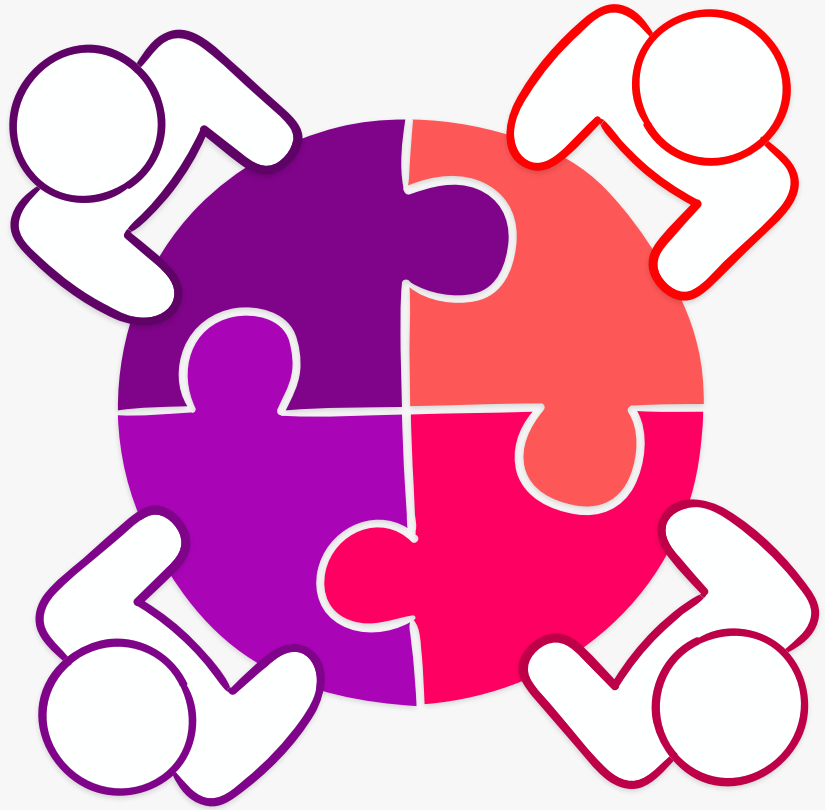
Click here to register

Reporting Lifecycle



Let's meet to discuss protecting your business

Schedule a meeting online or request a call back from our online calendar. Click HERE

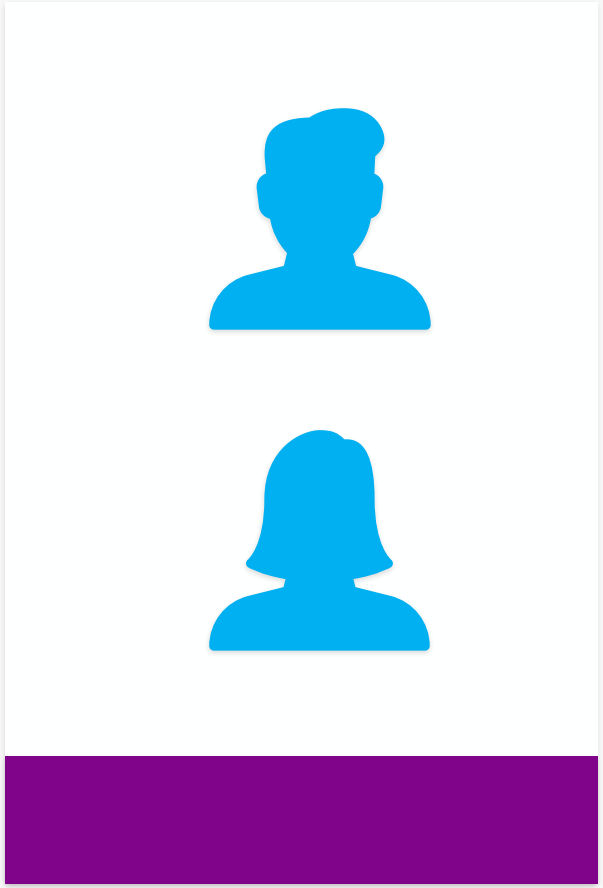


Let's protect your business against cyber attacks and data privacy breaches.

Let's connect

Facebook	Instagram	Twitter	LinkedIn
@g5cybersec	@g5cybersecurity	@g5cybersecurity	@g5cybersecurity
Click here to follow us	Click here to follow us	Click here to follow us	Click here to follow us

Thank you to everyone who contributed to making this report possible.



G5 Cyber Security

Thank you!

Please book a meeting for your business from our website.

g5cybersecurity.com