Country Travel Cyber Risk Report

October 2021

Cyberint

Executive Summary

Nowadays, as international travel – both for private and professional purposes – is a global standard, more and more organizations begin to recognize the ever-growing risk of cyber security threats which could target their employees as they travel abroad. Depending on the travel destination – in combination of various factors like the devices the employee takes with them on their trip – the risks to the employer range from harm to company devices to exposure of sensitive data.

In that context, Cyberint conducted an OSINT-based research to create a benchmark ranking countries according to the risk level they pose to organizations and their employees from a cyber-security perspective.

The scores calculated for each country in this report incorporate data from 3 main source types:

1. Global indexes for geographic cyber risk assessments
2. Data Records Breached Report
3. Global compromised machines analysis from Cyberint's own database

After consolidating inputs and data from the different sources, Cyberint provided a benchmark risk score in four different levels – Low, Medium, High, and Very High – to determine which are the safest countries for a traveler in terms of cyber risk:

Score Range	Risk Level
0-60	Very High
60-70	High
70-80	Medium
80-100	Low

The report details the main takeaways from the different databases used to calculate the scores. According to our analysis, the safest countries for travelers in terms of cyber security are Spain, France, Belgium, Austria and Italy, while the least safe are Jamaica, Colombia and Qatar.

Lastly, the report contains recommendations for action when traveling to each country, in terms of cyber security.

Data Sources

CYBERSECURITY EXPOSURE INDEX (CEI) 2020[1]

Cybersecurity Exposure Index (CEI) calculates the level of exposure to cybercrime by country from 0 to 100. The higher the score, the lower the exposure. Five data sets were used to create the Cybersecurity Exposure Index, measured in Windows defender and Bing Cloud services, each representing a different type of threat vector which could likely impact the particular user:

1. **Malware Encounter Rate by Microsoft (2019/20)[2]**
   Malware infection is often a result of poor security hygiene and minimal security education and awareness among users.

2. **Ransomware Encounter Rate (2019/20)**
   Attackers are shifting their efforts to customized campaigns—sometimes referred to as human operated ransomware—targeted at specific geographies, industries, and even individual businesses.

3. **Cryptocurrency Mining Encounter Rate (2019/20)**
   Attackers inject mining software into an unsuspecting user or organization's machine(s) and then use the machine's compute power to mine for the cryptocurrency.

4. **Drive-by Download Page Encounter Rate (2019/20)**
   A drive-by download (DBD) is a general term for any unintentional download of malicious code to an unsuspecting user's computer when they visit a website.

5. **Level of Commitment to Cybersecurity (2018)[3]**
   Each year, the level of commitment changes according to the information made available to the public, and through the different media and data provided by countries.

[1] https://passwordmanagers.co/cybersecurity-exposure-index/
[2] https://news.microsoft.com/wp-content/uploads/prod/sites/570/2020/02/Microsoft-Security-Endpoint-Threat-Summary-2019-Updated.pdf
[3] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

NATIONAL CYBER SECURITY INDEX (NCSI)[4]

The National Cyber Security Index is a global ranking scale which measures the preparedness of countries in preventing cyber threats and manage cyber incidents, **as reflected by each countries' regulation and legislation**. The NCSI also serves as a public database for evidence materials and as a tool for national cyber security capacity building.

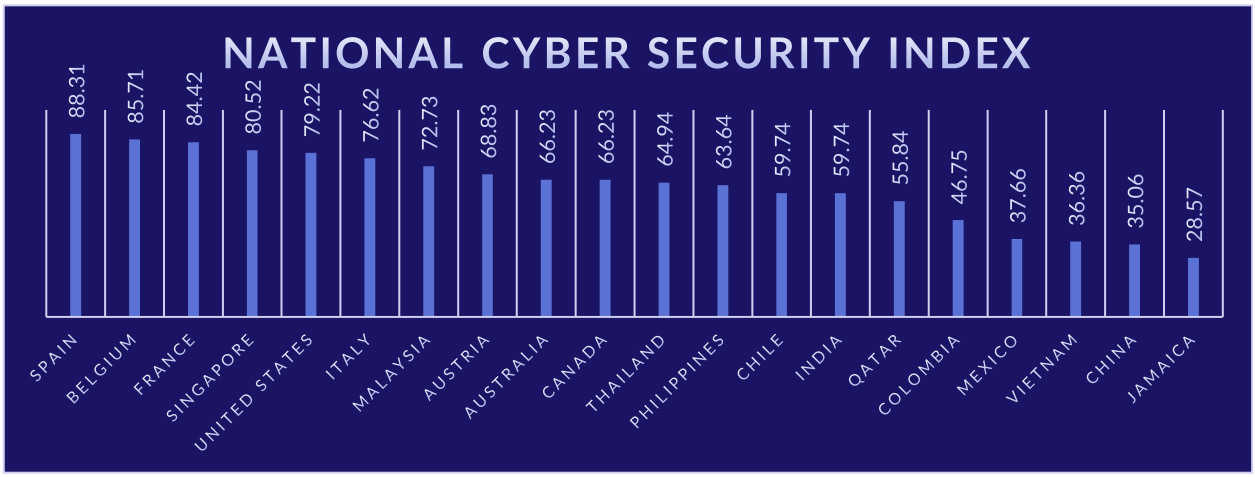
The NCSI Score shows the percentage the country received from the maximum value of the indicators. The maximum NCSI Score is always 100 (100%) regardless of whether indicators are added or removed; the higher the score – the lower the risk. The NCSI scoring is based on several components, out of which we emphasized 5 parameters for comparison:

Indicators of Public Infrastructure Cyber Security:

1. Protection of digital services – digital services providers are obligated to manage Cyber/ICT risks, and providers for the public sector are further subject to widely-recognized standards.
2. Protection of essential services – there is a state-appointed, competent supervisory authority in charge of regular monitoring of security measures for providers of critical services.
3. Protection of personal data – legislation and a supervisory authority are in place for protection of personal data.

Incident and Crisis Management Indicators:

4. Cyber crisis management – the government has established a crisis management plan for large-scale cyber incidents and assures that organizations participate in relevant exercises.
5. Fight against cybercrime - Cybercrimes are defined by law and enforced by a cybercrime unit.



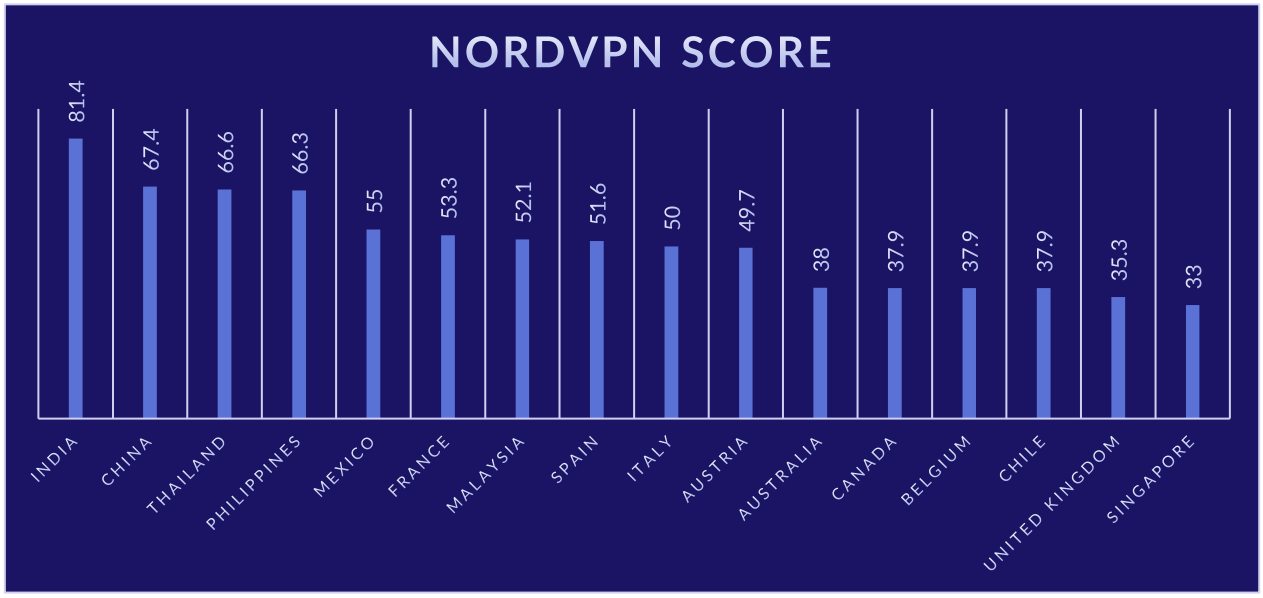
While not all the above parameters directly affect a casual traveller entering the destinations, they serve as indications for the overall maturity and awareness of those countries for cyber security risks, as well as the ability of the latter to support a traveller if they fall victim to such threats.

[4] **https://ncsi.ega.ee/**

NORDVPN CYBER RISK INDEX[5]

NordVPN's Cyber Risk Index (CRI) predicts the risk of becoming a victim of cybercrime depending on the country of residence; the higher the index – the lower the risk.

In this index, 50 countries comprising of 5.4 billion people are ranked according to 14 factors (2 are based on data collected in 2017, 5 on data collected in 2018, 4 on data collected in 2019, and 3 on data collected in 2020), including: Urban population, Monthly average wage, Tourism, Internet penetration, Smartphone penetration Time spent on the internet, E-commerce penetration, Online games penetration, VoD penetration, Public Wi-Fi availability, Facebook penetration, Instagram penetration, Crime Index, Global Cybersecurity index.



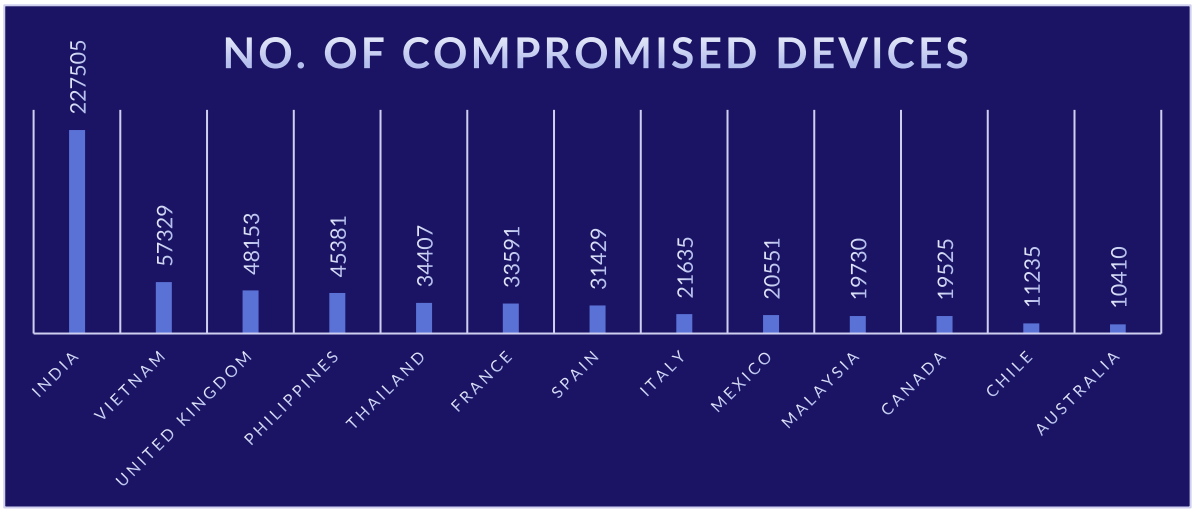
[5] **https://nordvpn.com/cri/**

DATA RECORDS LOST OR STOLEN BY COUNTRIES (BY VARONIS) 03/2020[6]

The number of lost or stolen data records varies from one country to another. The term "data records" refers to any piece of information that can put an individual or organization at risk, including email address, date of birth, account credentials, medical files, and banking details. In their analysis, Varonis used data from Thales' Breach Level Index,[7] and grouped the compromised records according to the locations of the organizations which reported them.

INFECTED MACHINES BY COUNTRY (CYBERINT ARGOS EDGE) 2017 - PRESENT

Cyberint collects logs from Command & Control servers of stealer malwares which infect machines around world. The metadata of each C&C malware log discloses the location of the infected machine. This allows Cyberint to analyze and identify the countries most affected from stealer malwares.



[6] https://www.varonis.com/blog/the-world-in-data-breaches/
[7] https://cpl.thalesgroup.com/data-threat-report

Cyberint Country Travel Cyber Risk (CTCR) Score Results

In calculating the CTCR score, Cyberint gave greater weight to the global indexes over the measures of Data Records and Compromised Devices, as they represent a wider variety of criteria. The full formula is as follows:

0.3 x CEI Score – Major Cyber Risk Index

+

0.3 x NCSI Score– Major Cyber Risk Index

+

0.3 x CRI Score - Major Cyber Risk Index

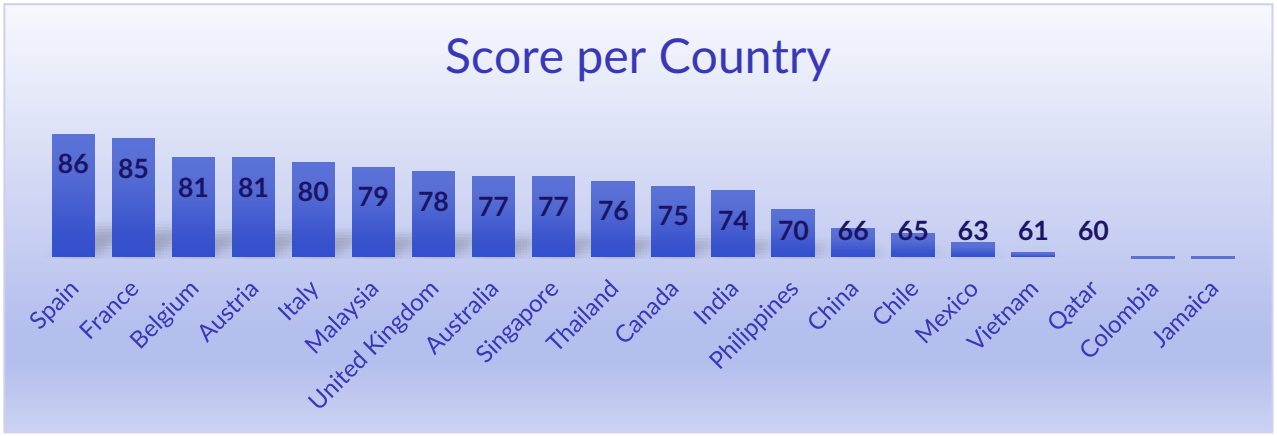
+

0.05 x (Data Records Lost Or Stolen/Population)[8]

+

0.05 x (Compromised Devices/Population)[9]

=



After calculating the score for each country, the scores were assigned risk levels as follows:

Score Range	Risk Level
0-60	Very High
60-70	High
70-80	Medium
80-100	Low

The higher the score – the safer the country from a cyber threat perspective.

[8] To represent a more realistically accurate calculation, the # of data records is divided by countries' population
[9] To represent a more realistically accurate calculation, the # of compromised devices is divided by countries' population

Country Travel Cyber Risk Assessment

Based on the above-detailed scores, the countries received the below risk level assessment:

Country	Total Score	Risk
Spain	86	Low
France	85	Low
Belgium	81	Low
Austria	81	Low
Italy	80	Low
Malaysia	79	Medium
United Kingdom	78	Medium
Australia	77	Medium
Singapore	77	Medium
Thailand	76	Medium
Canada	75	Medium
India	74	Medium
Philippines	70	Medium
China	66	High
Chile	65	High
Mexico	63	High
Vietnam	61	High
Qatar	60	High
Colombia	46	Very High
Jamaica	29	Very High

Disclaimer:

Throughout the research Jamaica, Qatar and Vietnam lacked the index score in one or more of the data sources, thus, all three countries received a score of 0 in each missing specific parameter, which impact their overall score.

One of main parameters we took into consideration is how accessible and sharable cyber security measures and protocols are. In case one's cyber security measures and protocols are consistently lacking in sharing – it should raise immediate suspicion and awareness.

In addition, to date, Taiwan is not indexed in the mentioned sources, due to this fact we could not determine Taiwan's score and d recommend being cautious while traveling to Taiwan.

Based on the risk level assigned to each country, a traveler may consider applying different levels of protection steps or cyber safety guidelines; see in the below chapter.

Cyber Security Guidelines for Travelers Per Risk Level

Country's Risk Level\ Activities	Wireless Communications (Public Wi-Fi, Bluetooth etc.)	Using Financial Services (ATM, Exchange etc.)	Using Public or Local Technological Services (Shared Computers, USB Device, Installing Local Apps etc.)
Very High	Not Recommended	Not Recommended	Not Recommended
High	Not Recommended	Not Recommended	Not Recommended
Medium	Safe	Safe	Not Recommended
Low	Safe	Safe	Not Recommended

General Cyber Travel Recommendations

Before traveling:

1. Inquire after your organization's hardware and software travel policies.
2. Make sure your devices are protected with a PIN, passphrase, or password.
3. Enable multi-factor authentication wherever available, to help prevent threat actors who may steal your devices from taking over your accounts and accessing your data.
4. Back up your data files to another device or to software, such as Dropbox or a cloud storage program.
5. Make sure you have protection software on your devices (Anti-Virus, etc.) and that those are up to date.

During the trip:

1. Avoid using public workstations
2. Mind your surroundings when logging in or inputting data into your devices.
3. Disable your Wi-Fi connection when you are not using your device to connect to the Internet.
4. **Never connect an unknown device to your tablet or laptop**. Any unfamiliar device that connects to a USB port (flash drive, MP3 players, smart phones, external hard drives, etc.) can be considered a storage device and may contain malicious software.
5. Always keep your devices with you. Don't leave your phone charging in a public conference room while you go for lunch or lend your phone to a stranger who needs to make a call.
6. Avoid leaving valuable or sensitive electronic equipment in your hotel room. If you must, remove the battery, if possible, and the SIM card and keep them with you.
7. Power off devices while going through customs or other inspection points.

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City