INDUSFACE™

2023

Safest Countries for Remote Work in 2023

Recent research has shown that 68% of high-revenue growth companies have embraced a hybrid model worldwide. With businesses enjoying remote or hybrid working, benefits including reduced maintenance costs, improved flexibility, and an extended talent pool, cybersecurity awareness has become more critical than ever.

With this in mind, Indusface is intrigued to find **the most secure countries for businesses to allow their employees to work from** by creating an index score based on cybersecurity data, including DDoS attacks, phishing sites, malware-hosting sites, and compromised computers. Venky Sundar, Founder and President of Indusface, also provides **six tips for small businesses on ensuring cybersecurity.**

KEY FINDINGS:

- Honduras is named the most cyber secure country for businesses across the world to allow their employees to work from, with a cybersecurity index score of 89.55 out of 100.
- South Korea and Japan occupy the second and third places worldwide in terms of cybersecurity, scoring 88.88/100 and 87.49/100, respectively.
- India ranked 12th most cyber secure country in Asia and only 45th in the world, with a cybersecurity score of just 70.09/100.
- Cyprus is the world's least cyber secure country, with an index score of 43.19/100.
- Venky Sundar, Founder and President of Indusface, provides 6 top tips for cybersecurity when working remotely.

INDIA RANKED 12TH AS THE MOST CYBER SECURE ASIAN COUNTRY

Indusface found out that India **ranked 12th most cyber secure Asian country and the 45th in the global ranking,** with an overall cybersecurity index score of 70.09/100! Despite having the lowest incidence of DDoS attacks, at a rate of only 3 per 100,000 Internet users, India possesses a considerable number of phishing (490) and malware-hosting (1360) sites per 100,000 URLs, resulting in a diminished cybersecurity score on a global scale.

Please find the complete data, including all countries, here.

Top 10 most cyber secure countries to work from

Rank	Country	DDoS attacks per 100,000 Internet Users	Phishing sites per 100,000 URLs	Malware hosting sites per 100,000 URLs	Compromised computers per 100,000 Internet users	Cyber security index score (/100)
1	Honduras	40	90	120	413	89.55
2	South Korea	59	100	560	13	88.88
3	Japan	12	150	730	21	87.49
4	Costa Rica	41	180	270	712	84.87
5	Guatemala	112	20	300	516	84.48
6	Mexico	27	80	350	1,948	84.31
7	Colombia	19	180	440	1,073	82.67
8	Belgium	79	320	430	47	82.49
= 9	Ecuador	51	170	330	1,349	82.48
= 9	Finland	314	280	390	11	82.48

* Total DDoS Attacks were counted between 2015 to 2021.

**Compromised computers = have been infected with the Gamarue botnet. Please see the full methodology below

INDUSFACE

discovered **that Honduras earns the title of the world's most secure country for businesses to allow employees to remotely work from, with a cybersecurity score of 89.55 out of 100.**

Securing the second position with a score of **88.88** out of 100, **South Korea** emerges as the leading choice for businesses to permit their employees to work remotely.

Honduras received the **fourth lowest** number of DDoS attacks **(40)** from 2015 to 2021, with only 28 attacks higher than Japan, with the lowest among the top 10 countries. This is an important factor for businesses to consider, as successful DDoS attacks could block your business sites and bring down all servers and connections you depend on.

Contributing to **South Korea's** top ranking is that it has the second lowest number of compromised computers per 100,000 internet users **(13)** in the country.

Computers infected with the Gamarue botnet open doors for hackers and make it easier for them to take control of your business data and devices. Honduras also has the joint lowest malware-hosting sites among all the top 10 countries, with an average of **120** sites per 100,000 URLs.

Japan is ranked third as the most cyber secure country, **with an overall cybersecurity index score of 87.49/**100. Boasting the lowest number of phishing sites **(20)** per 100,000 URLs and malware-hosting sites **(300), Guatemala** owns fewer sites that could trick you or contain malware, making businesses less worried about stolen sensitive information.

In **fourth** place is **Costa Rica,** with a cybersecurity index score of **84.87**/100. **Guatemala** and **Mexico** hold the fifth and sixth positions, scoring **84.48**/100 and **84.31**/100, respectively.

5 Least cyber secure countries to work from

Rank	Country	DDoS attacks per 100,000 Internet Users	Phishing sites per 100,000 URLs	Malware hosting sites per 100,000 URLs	Compromised computers per 100,000 internet users	Cyber security score (/100)
1	Cyprus	404	1730	1280	400	43.19
2	Panama	191	1560	1150	461	48.50
3	Tunisia	429	310	930	5,588	50.97
4	Bulgaria	167	1220	1,170	430	51.82
5	Serbia	174	780	790	1467	53.85

Cyprus ranks as the **least secure country** in the world for businesses to allow employees to work remotely, with a total cybersecurity score of only **43.19** out of 100. With **1,730** phishing sites and **1,280** malware-hosting sites per 100,000 URLs, businesses in the country will need to be extra careful when identifying whether a website is genuine.

Panama owns one of the highest numbers of phishing site URLs **(1560)** per 100,000 internet users, leading to its low cybersecurity score of **48.50** / 100 - ranking as the second least cyber secure country across the world.

VENKATESH SUNDAR, FOUNDER AND PRESIDENT OF INDUSFACE, COMMENTS ON WORKING REMOTELY ACROSS THE WORLD:

"Attracting top talent through remote work can revolutionize your business. However, it also leaves your sensitive data and assets vulnerable to hackers. Therefore, it is important to be prepared to address remote work security risks. There are a few points when recruiting talents globally:

Firstly, you could consider which countries are least targeted by hackers and least risk to your cybersecurity.

Secondly, look at regulations that govern data security. For example, GDPR is probably the gold standard when it comes to data security.

Thirdly, research law enforcement. This indicates how quickly people will be punished when committing cybercrime.

Fourthly, get to know the government grants. Cybersecurity grants are provided to SMBs who tend to be more susceptible to attacks.

Fifthly, the level of cybersecurity awareness in the generation also affects how likely hackers would commit cybercrimes."

VENKATESH SUNDAR, FOUNDER AND PRESIDENT OF INDUSFACE, PROVIDES SIX TOP TIPS FOR BUSINESSES WHO APPLY FOR REMOTE OR HYBRID WORKING:

"There is no one way to secure remote working, but instead, you should make remote work access security an integral part of your employee's ongoing training and workplace culture. Here are six best practices for secure remote working within your business:

01 *Create strong authentication*

It starts by identifying the remote worker before a worker can access corporate data and assets. From this, you can build audit trails of the actions against the identity.

02 *Update your systems and encrypt your devices*

Outdated technology could open doors for hackers with credential information like credit cards being stolen. Cases like this will have a fatal hit on your business's reputation as well as cybersecurity. It is highly recommended that all your devices be updated and encrypted with SSL certificates.

03 *Detect Security Weaknesses with DAST*

Human error accounts for 95% of security breaches; the sooner a vulnerability is caught, the cheaper it is to fix. By leveraging a DAST scanner, you can identify application vulnerabilities and promptly notify remote workers, including instances of weak passwords being utilized.

04 *Deploy Web Application Firewall*

WAF evaluates every request to identify potential threats or abnormal activities. With WAF, you can bolster the security of remote work by mitigating web-based threats, securing application layers, detecting anomalies, and providing virtual patches.

05 *Automate Asset Discovery*

Remote and hybrid workforces have expanded the attack surface, presenting hackers with new points of entry into network environments. Asset discovery plays a pivotal role in attack surface management. Automate asset discovery to identify shadow IT systems, vulnerabilities, and connected risks.

06 *Malware and DDoS Attack Monitoring*

Attackers leverage malware to infect and hijack machines and devices, empowering them to execute DDoS attacks. Monitor your network traffic for abnormalities or spikes in traffic to drop the DDoS attack and handle malware propagation, intrusion activities, and malicious threats like SQL Injection and XSS.

METHODOLOGY

Indusface conducted the following research and analyzed historical cyberattack data per country to find the most secure countries to work from:

1. Firstly, detected cyberattacks between 2015-2021 were sourced from the Digital Attack Map. The dataset was subsequently cleaned and aggregated by country to find the total number of attacks and the distribution of attacks by attack type.

2. Then, Python data mining tools were used to extract cybersecurity statistics from over 90 Microsoft Security Intelligence reports (2017), resulting in a comprehensive dataset containing the number of phishing sites, malware-hosting sites, and compromised computers (part of gamarue botnet).

3. Phishing and malware-hosting sites data collected above were presented on a per 100,000 URLs basis, and compromised computers and DDoS attacks were presented per 100,000 internet users .

4. An index score of cybersecurity was then computed, considering the above three factors to assess the favourability of each country as a workstation destination.

5. **The data was collected in June 2023 and is correct as of then.**