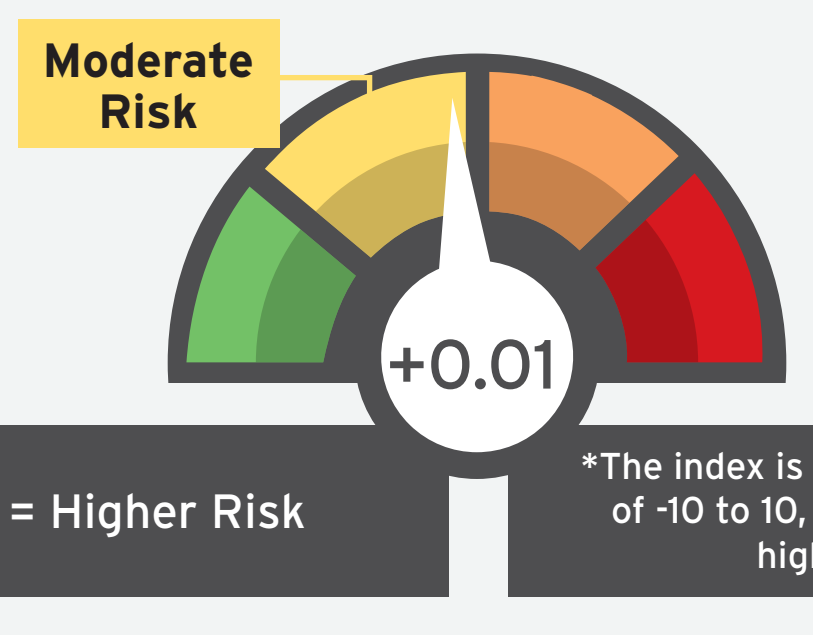
CYBER RISK INDEX (CRI)

With cyberattacks a constant threat, it's crucial for companies to focus on assessing, detecting, preventing, and responding to today's cyber threats. In this iteration of the CRI, performed in 2H'2022, Trend Micro and Ponemon Institute conducted research among IT managers across Europe, Asia-Pacific, Latin/South America, and North America. These findings are used to create a comprehensive index to assess an organization's cyber risk maturity level. For the first time, the global cyber risk index turned positive and rose into the moderate risk level.

Current global cyber risk level:



Lower CRI = Higher Risk

*The index is based on a numerical scale of -10 to 10, with -10 representing the highest level of risk.

Top risk factors in the 2H'2022

In the 2H'2022, the risk level improved from -0.15 to +0.01 since the previous survey. This means respondents feel their risk improved when preparing for cyberattacks and they felt a lower risk also from the current threats targeting them.

Cyber Risk Index Elevated Risk

Data Risk

Top Data Types at Risk:
1. Business communication (email)
2. Human resource (employee) files
3. Financial information
4. R&D information
5. Company-confidential information

Data Risks
- My organization is not well prepared to deal with data breaches and cybersecurity exploits.
- My organization's IT security function is not able to prevent most cyberattacks
- My organization's IT security function is not able to detect zero-day attacks

Cyber Risk

Cyber Risks:
1. Clickjacking
2. Business Email Compromise (BEC)
3. Ransomware
4. Fileless attack
5. Botnets

Infrastructure Risk

Top Security Risks Within IT Infrastructure:
1. Negligent insiders
2. Cloud computing infrastructure and providers
3. Mobile/remote employees
4. Shortage of qualified personnel
5. Virtual computing environments (servers, endpoints)

Infrastructure Risks:
- My organization's IT security function does not have the ability to know the physical location of business-critical data assets and applications.
- My organization's IT security objectives are not aligned with business objectives.

Human Capital Risk

Human Capital Risks:
- My organization's CEO and Board of Directors are not actively involved in overseeing the IT security function.

Human Capital Risks:
- My organization's senior leadership doesn't view security as a competitive advantage.

Operational Risk

Top negative consequences of cyberattacks:
1. Disruption or damages to critical infrastructure
2. Productivity decline
3. Cost of outside consultants and experts
4. Regulatory actions or lawsuits
5. Reputation or brand damage

Operation Risks:
- My organization's IT security function hasn't the ability to unleash countermeasures (such as honeypots) to gain intelligence about the attacker.
- My organization's IT security architecture doesn't have high interoperability, scalability, and agility.

Cyber Risk Index

This index measures the difference between the Cyber Preparedness Index and the Cyber Threat Index. In other words, the divide between an organization's current security posture and their likelihood of being attacked.

Region: North America, Latin/South America, Europe, Asia-Pacific, All Regions (scale -10 to 0 to 10)

Region	2H'2022	1H'2022	2H'2021	Level
North America	-0.10	-0.33	-0.01	Elevated
Latin/South America	-0.03	-0.03	-0.20	Elevated
Europe	+0.12	-0.12	-0.15	Moderate
Asia-Pacific	+0.05	-0.11	+0.20	Moderate
All Regions	+0.01	-0.15	-0.04	Moderate

Moderate risk level for cyber preparedness index

North America has the highest overall risk, due to less preparedness and a higher threat concern than the other three regions

Elevated risk level in cyber threat index

Breakdown of Cyber Risk Index

The Cyber Preparedness Index is at a moderate risk for all regions with Latin/South America being at the highest risk level.

Overall, all organizations are at a moderate cyber risk.

All organizations show an elevated risk associated with the Cyber Threat Index, with all regions exhibiting approximately the same level of risk, but Asia-Pacific has the highest risk level.

Cyber Preparedness Index

Lower number, higher risk

North America	Latin/South America	Europe	Asia-Pacific	All Regions
5.29	5.22	5.39	5.47	5.34

Cyber Preparedness Index Ratings

Range	
7.51 to 10	Low Risk
5.01 to 7.50	Moderate Risk
2.51 to 5.0	Elevated Risk
0 to 2.5	High Risk

Cyber Threat Index

Higher number, higher risk

North America	Latin/South America	Europe	Asia-Pacific	All Regions
5.39	5.25	5.27	5.42	5.33

Cyber Threat Index Ratings

Range	
7.51 to 10	High Risk
5.01 to 7.50	Elevated Risk
2.51 to 5.0	Moderate Risk
0 to 2.5	Low Risk

Differences Between Regions

Top 5 cyber threats

All Regions
1. Clickjacking
2. Business Email Compromise (BEC)
2. Ransomware
4. Fileless Attack
5. Botnets

North America
1. Fileless Attack
2. Man-in-the-Middle Attack
3. Malicious Insiders
4. Business Email Compromise (BEC)
5. Watering Hole Attacks

Latin/South America
1. Clickjacking
2. Fileless Attack
3. Business Email Compromise (BEC)
3. Login Attacks (Credential Theft)
3. Ransomware

Europe
1. Clickjacking
2. Login Attacks (Credential Theft)
3. Ransomware
4. Botnets
5. Crypto Mining

Asia-Pacific
1. Business Email Compromise (BEC)
2. Ransomware
3. Clickjacking
4. Botnets
5. Crypto Mining

Likelihood of a successful cyberattack

Across the four regions, respondents are concerned they will be successfully attacked in the next 12 months. **72% in North America** and **83% in Europe**, **82% in Asia-Pacific**, and **77% in Latin/South America** responded as somewhat to very likely to be compromised in the next 12 months.

North America

Latin/South America

Europe

Asia-Pacific

Key Survey Questions

Several key survey questions were asked to IT managers to measure important aspects of their companies' cybersecurity posture. Here's a sampling of the survey's more revealing questions

1 My organization's IT security function has the ability to know the physical location of business-critical data assets and applications. (Lower number means less prepared on 0-10 point scale)

North America	Latin/South America	Europe	Asia-Pacific
4.89	4.59	4.38	4.68

Likelihood of a data breach of critical data (IP) in next 12 months: 69% likelihood

TAKEAWAY

With 7 out of 10 surveyed saying a breach of critical data is likely in the next 12 months, and a lack of preparedness to deal with an attack, organizations should rethink their current security strategy.

2 How many separate cyberattacks that infiltrated your organization's networks and/or enterprise systems did your organization experience over the past 12 months? Below shows percentage of those with one or more attacks.

North America	Latin/South America	Europe	Asia-Pacific
78%	89%	84%	87%

Likelihood of one or more successful cyberattacks in the next 12 months globally: 78% likelihood

TAKEAWAY

Nearly 8 out of 10 say they are likely to be breached in the next 12 months, and as such, organizations need to build improved breach detection capabilities.

3 The percentage of organizations who had seven or more separate cyberattacks over the past 12 months.

North America	Latin/South America	Europe	Asia-Pacific
34%	35%	29%	32%

The top four data types at highest risk of loss or theft are:

- Business communication (email)
- Human resource (employee) files
- Financial information
- R&D information

TAKEAWAY

The top four data types at risk cited by respondents are critical to a business' operations and livelihood.

TREND MICRO™