The 2H'2022 Cyber Risk Index (CRI)

Trend Micro, in conjunction with Ponemon Institute, presents the seventh edition of the Cyber Risk Index (CRI). This comprehensive index aims to measure an organization's readiness to respond to different types of cyberattacks.

The 2H'2022 version of the CRI was developed from a survey conducted by Ponemon Institute. This includes more than 3,700 CISOs, IT practitioners, and managers across the regions of North America, Europe, Latin/South America, and Asia-Pacific.

The CRI is calculated by subtracting the cyber threat index from the cyber preparedness index. The scale ranges from +10 to -10, with -10 representing the highest risk.

The CRI is composed of two individual indices:

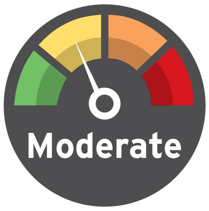
- **Cyber preparedness index**: Representing an organization's readiness to defend against cyberattacks.
- **Cyber threat index**: The state of the threat landscape at the time the CRI was determined.

CYBER RISK INDEX RATINGS		
Range	Color Code	Interpretation
5.01 to 10.00	🟩	Low Risk
0.01 to 5.00	🟨	Moderate Risk
0.00 to -5.00	🟧	Elevated Risk
-5.01 to -10.00	🟥	High risk

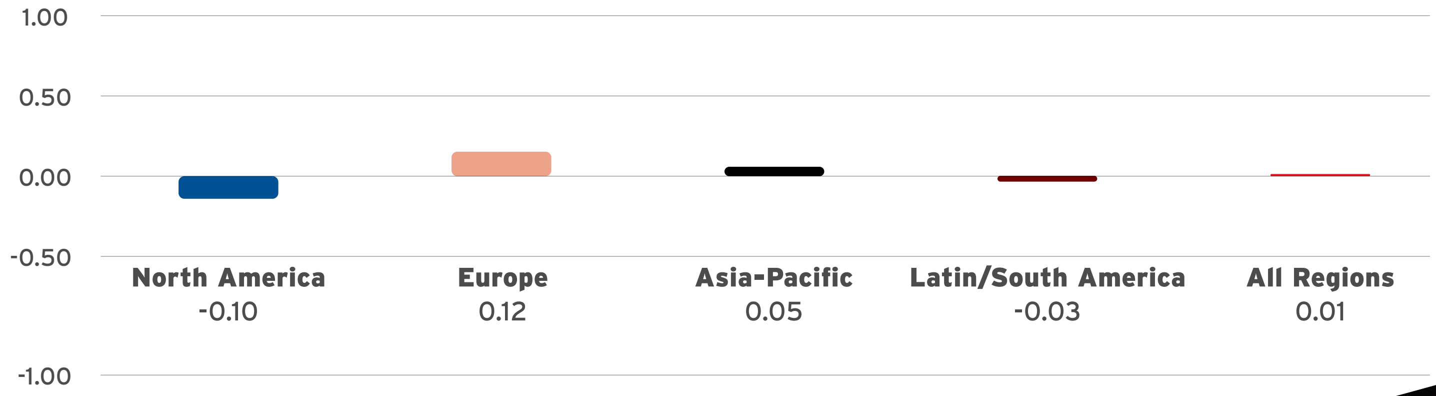
CYBER PREPAREDNESS INDEX RATINGS			CYBER THREAT INDEX RATINGS		
Range	Color Code	Interpretation	Range	Color Code	Interpretation
7.51 to 10.00	🟩	Low Risk	7.51 to 10.00	🟥	High Risk
5.01 to 7.50	🟨	Moderate Risk	5.01 to 7.50	🟧	Elevated Risk
2.51 to 5.00	🟧	Elevated Risk	2.51 to 5.00	🟨	Moderate Risk
0.00 to 2.50	🟥	High Risk	0.00 to 2.50	🟩	Low risk

GLOBAL CYBER RISK INDEX

+0.01



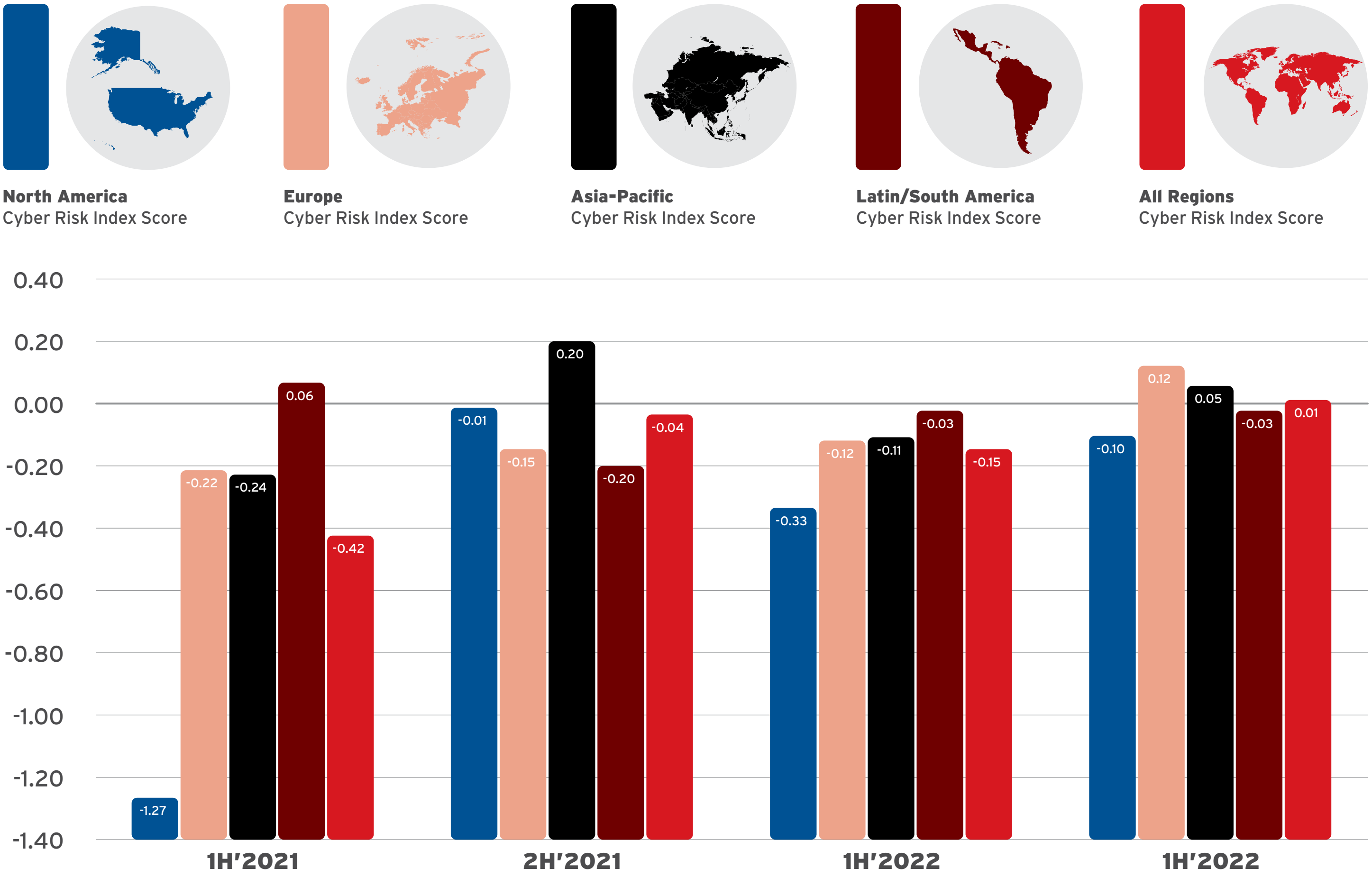
REGIONAL CYBER RISK INDEX 2H'2022



In this latest global survey from 2H'2022, we saw the cyber risk index move positive to +0.01 which brought the risk level into the moderate range. This means that, globally, most organizations feel their cyber risk has improved since the 1H'2022 survey when it was -0.15. If we look at the above chart, you can see that both the Europe and Asia-Pacific regions are also in the moderate risk level with +0.12 and +0.05 respectively. North America and Latin-South America remained in the elevated risk levels at -0.10 and -0.03, with North America improving their cyber risk since the 1H'2022 and Latin-South America remaining the same level. (See below trending chart.)

If we look further into the global results, we see the cyber threat index decreased from 1H'2022 to 2H'2022 (5.39 to 5.33). For the threat index, this lower number means lower risk. The cyber preparedness index saw a improvement too, rising from 5.24 to 5.34 between the 1H'2022 to 2H'2022 survey results, and this higher number means lower risk as well. The good news is that organizations are making changes to improve their preparedness against attacks. We will see if this trend continues in 2023, where we will be shifting to a once yearly release of the survey.

CYBER RISK INDEX TRENDS



THE PRIMARY BUSINESS RISKS

The top cybersecurity risk factors businesses face can be broken down into five categories, based on the top concerns from respondents across the four regions:

- Top cyber threats (the top four remained from the last survey, but botnets replaced login attacks)
    1. Clickjacking
    2. Business Email Compromise (BEC)
    2. Ransomware
    4. Fileless attack
    5. Botnets
- Top data types at risk (The last two tied in preparedness score)
    o "My organization is not well-prepared to deal with data breaches and cybersecurity exploits"
    o "My organization's IT security function is not able to prevent most cyberattacks"
    o "My organization's IT security function is not able to detect zero-day attacks"
- Human capital risk
    o "My organization's senior leadership doesn't view security as a competitive advantage"
    o "My organization's CEO and board of directors are not actively involved in overseeing the IT security function"
- Top infrastructure risks (the top 3 remained from 1H'2022, but 4 and 5 are new this round)
    1. Negligent insiders
    2. Cloud computing infrastructure and providers
    3. Mobile/remote employees
    4. Shortage of qualified personnel
    5. Virtual computing environments (servers, endpoints)
- Operational risk
    o "My organization's IT security function doesn't have the ability to unleash countermeasures (such as honeypots) to gain intelligence about the attacker"
    o "My organization's IT security architecture doesn't have high interoperability, scalability, and agility"

WHAT BUSINESSES STAND TO LOSE

While any information a business possesses is prone to data loss or theft, these five information types are the ones that present the greatest risk for an organization—based on results from the survey. In this survey the top 3 remained from the last survey in 1H'2022, and 4 and 5 are new to the top 5 list.

1. Business communication (email)
2. Human resource (employee) files
3. Financial information
4. R&D information
5. Company-confidential information

In looking at the above results, it is clear that organizations put the most emphasis on the data that could cause repercussions for the employee or business if it was stolen or compromised.

Top concerns (negative consequences) of a successful cyberattack are:

- Disruption or damages to critical infrastructure
- Productivity decline
- Cost of outside consultants and experts
- Regulatory actions or lawsuits
- Reputation or brand damage

THE GREATEST CYBERSECURITY CHALLENGES FOR BUSINESSES

The polled organizations determined their risk factors based on the effectiveness of their security functions. Based on the global survey results, these are the greatest preparedness areas of concern for businesses:

- **People**: "My organization's senior leadership does not view security as a competitive advantage"
- **Process**: "My organization's IT security function doesn't have the ability to unleash countermeasures (such as honeypots) to gain intelligence about the attacker"
- **Technology**: "My organization's IT security function does not have the ability to know the physical location of business-critical data assets and applications"

PROTECTING BUSINESSES FROM CYBER THREATS

Taking the current threat landscape into consideration and based on the CRI findings, global businesses can still effectively minimize their risks by implementing security best practices. These include:

- Identifying and building security around critical data by focusing on risk management and the threats that could target this data
- Implementing attack surface discovery to identify both internal and external systems, accounts, and devices that you have
- Minimizing infrastructure complexity and improving alignment across the whole security stack
- Getting senior leadership to view security as a competitive advantage
- Improving the ability to protect the business environment, including properly securing bring your own device (BYOD), internet of things (IoT), and industrial IoT devices (IIoT), as well as cloud infrastructure
- Investing in both new talent and existing security personnel to help them keep up with the rapidly evolving threat landscape, as well as improve retention
- Reviewing existing security solutions with the latest technologies to detect advanced threats like ransomware and botnets
- Improving IT security architecture with high interoperability, scalability, and agility
- Discuss with your security partner how a unified cybersecurity platform that includes extended detection and response (XDR) capabilities to improve your visibility and response to attacks

Key takeaways for businesses

Our findings show that global businesses have a very high chance of being affected by a cyberattack, with eight out of 10 thinking they will be successfully attacked in the next 12 months.

- Likelihood of a data breach of customer data in the next 12 months: **70%**.
- Likelihood of a data breach of critical data (IP) in the next 12 months: **69%**.
- Likelihood of one or more successful cyberattacks in the next 12 months: **78%**.

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy