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

The 2H’2021 version of the CRI was developed from a survey conducted by Ponemon Institute. This includes more than 3,400 CISOs, and IT practitioners and managers across the regions of North America, Europe, Latin/South America, and Asia-Pacific.

Three of four regions show an elevated risk (negative CRI number), with Latin/South America having the highest risk level compared to the other three regions. This is due to Latin/South America having a lower perceived readiness than the other regions. Asia/Pacific has a positive CRI (moderate risk) due to improved preparedness and perception that the threat landscape has improved.

The CRI is composed of two individual indices:

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

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

### CYBER RISK INDEX 2H’2021

<table>
<thead>
<tr>
<th>Region</th>
<th>CRI Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>-0.01</td>
</tr>
<tr>
<td>Europe</td>
<td>-0.15</td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>0.20</td>
</tr>
<tr>
<td>Latin/South America</td>
<td>-0.20</td>
</tr>
<tr>
<td>All Regions</td>
<td>-0.04</td>
</tr>
</tbody>
</table>
The past three CRI editions have included North America, Europe, and Asia-Pacific with Latin/South America included in last two. As you see below, other than Latin/South America, the CRI has improved (lower risk) in the other three regions. This is mainly due to improved cyber preparedness and a lower cyber threat index. Many of the changes were due to effects of the pandemic and shifts in organizations supporting more work-from-home (WFH) employees while accelerating their cloud adoption.

**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 five cyber threats**
1. Ransomware
2. Phishing and social engineering
3. Denial of service (DoS)
4. Botnets
5. Man-in-the-middle attack

**Top five data types at risk**
- “My organization is not well prepared to deal with data breaches and cybersecurity exploits”
- “My organization's enabling security technologies are not sufficient to protect data assets and IT infrastructure”
- “My organization's IT security function is not able to contain most cyber attacks”

**Human capital risk**
- “My organization's IT security leader (CISO) doesn't have sufficient authority and resources to achieve a strong security posture”
- “My organization's IT security leader does not report to senior leadership (such as the CEO, COO, or CIO)”
- “My organization's IT security personnel do not have sufficient knowledge, skill, and expertise to protect data assets and IT infrastructure”

**Top five infrastructure risks**
1. Mobile/remote employees
2. Cloud computing infrastructure and providers
3. Across third-party applications
4. Malicious insiders
5. Mobile devices, such as smart phones

**Operational risk**
- “My organization's IT security function lacks support of security in the DevOps environment”
- “My organization's IT security function does not strictly enforce acts of non-compliance to security policies, standard operating procedures, and external requirements”
- “My organization's IT security function lacks compliance with data protection and privacy requirements”

---

**REGIONAL CYBER RISK INDEX TRENDS**

![Bar chart showing regional cyber risk index scores for 2020, 1H'2021, and 2H'2021.](chart_image)
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.

1. R&D information
2. Financial information
3. Business communication (email)
4. Company-confidential information
5. Trade secrets

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

Top concerns (negative consequences) of a successful cyber attack are:
- Stolen or damaged equipment
- Cost of outside consultants and experts
- Customer turnover
- Reputation or brand damage
- Regulatory actions or lawsuits

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 IT security leader (CISO) does not have sufficient authority and resources to achieve a strong security posture”
- **Process**: “My organization’s IT security function lacks enforcement on acts of non-compliance to security policies, standard operating procedures, and external requirements”
- **Technology**: “My organization does not make appropriate investments in leading-edge security technologies, such as machine learning, automation, orchestration, analytics, and/or artificial intelligence (AI) tools”

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
- Implement attack surface discovery to identify both internal and external systems, accounts, 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), and 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 (Note, these are all down from the previous CRI survey in 1H'2021).

- Likelihood of a data breach of customer data in the next 12 months: **67%**
- Likelihood of a data breach of critical data (IP) in the next 12 months: **71%**
- Likelihood of one or more successful cyberattacks in the next 12 months: **76%**