THE 1H'2021 CYBER RISK INDEX (CRI)

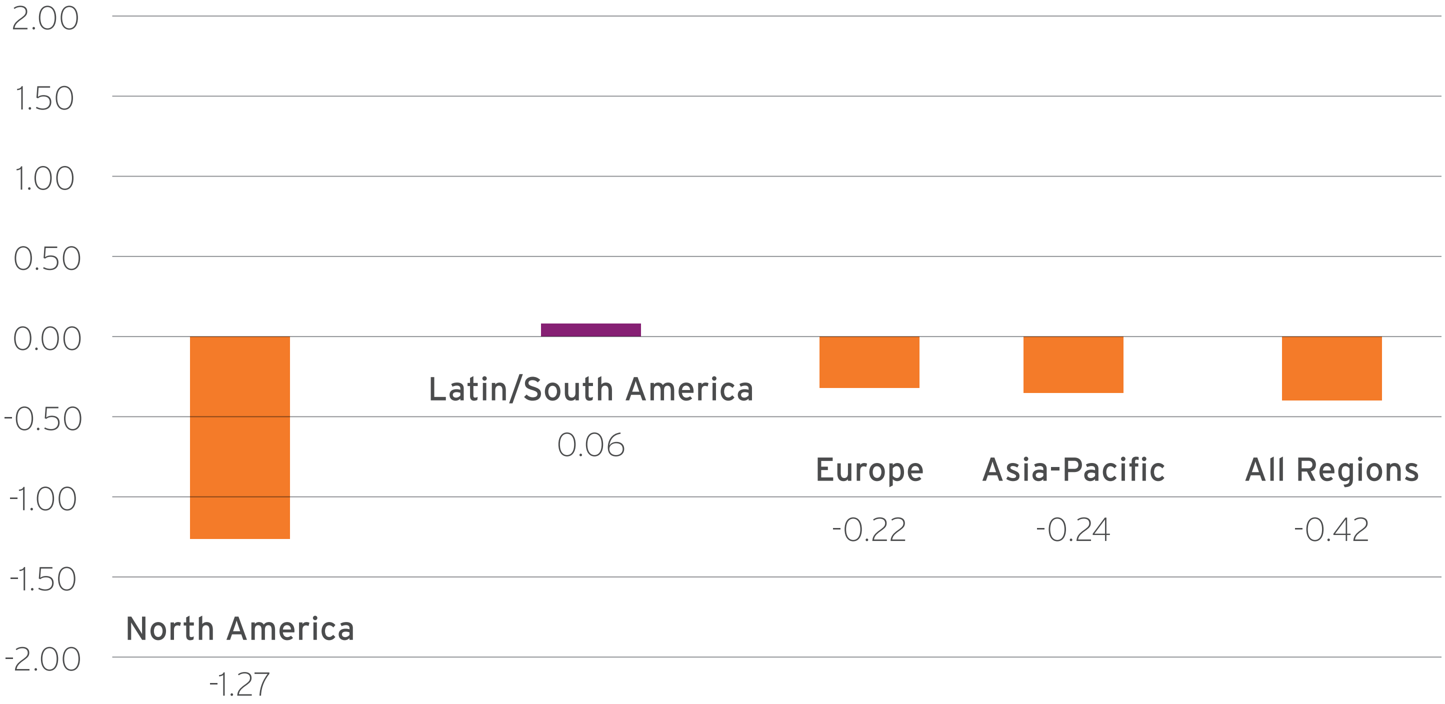
Trend Micro, in conjunction with Ponemon Institute, presents the fourth edition of the Cyber Risk Index (CRI). This comprehensive index aims to measure an organization's readiness to respond to different kinds of cyberattacks.

The 1H'2021 version of the CRI was developed from a survey conducted by Ponemon Institute, which included more than 3,600 CISOs, IT practitioners, and managers across North America, Europe, Latin/South America, and Asia-Pacific.

The CRI is composed of two individual indices:

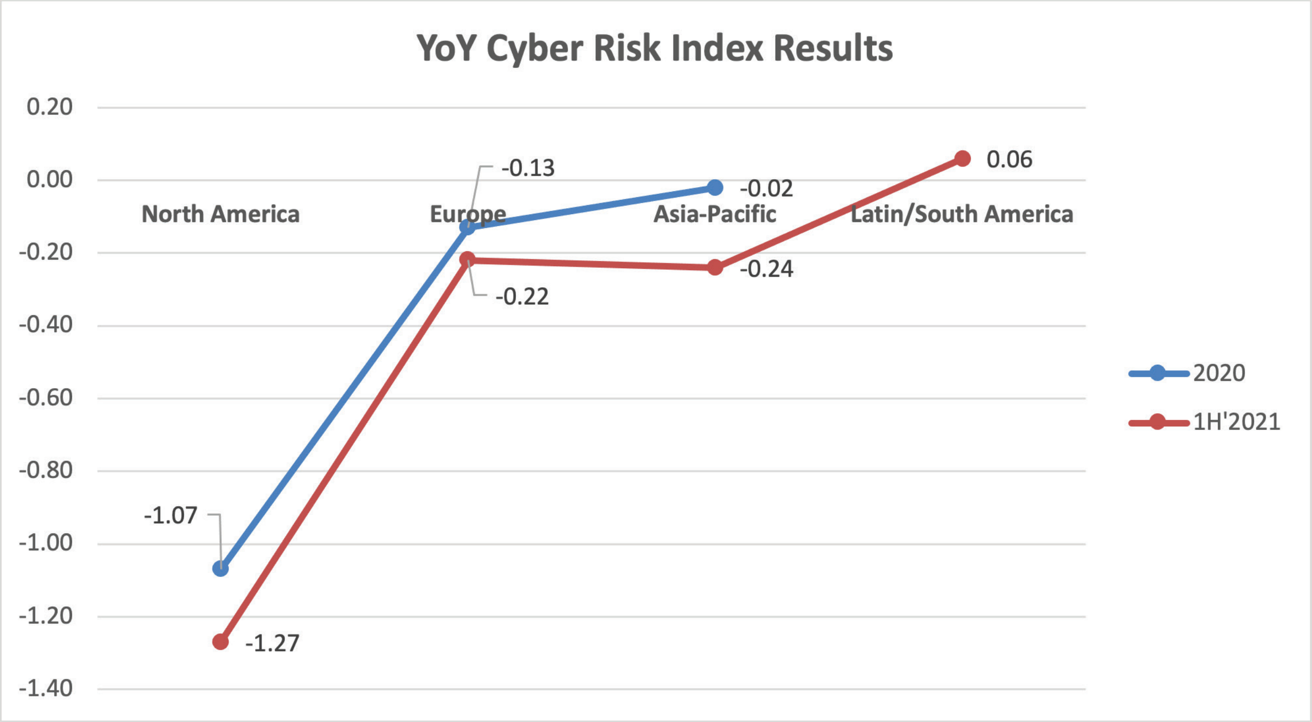
- **Cyber Preparedness Index**–representing an organization's readiness to defend against cyberattacks
- **Cyber Threat Index**–the state of the threat landscape at the time the CRI was determined

CYBER RISK INDEX 1H'2021



Three of four regions showed an elevated risk (negative CRI number), with North America having the highest risk level compared to the other three regions. This was due to North America having a lower perceived readiness than the other regions.

The past two CRI editions have included North America, Europe, and Asia-Pacific. As you see below, the trend has been greater risk (more negative number) across the three regions, mainly due to concerns the threats are getting worse.



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:

Cyber Threat Risk

1. Man-in-the-middle attacks
2. Ransomware
3. Phishing and social engineering
4. Fileless attack
5. Botnets

Data Risk

- My organization's IT security function is not able to prevent most cyberattacks.
- My organization's IT security function is not able to detect most cyberattacks.
- My organization's IT security function is not able to detect zero-day attacks.

Human Capital Risk

- My organization's IT security leader (CISO) does not have the sufficient authority and resources to achieve a strong security posture.
- My organization's C-level executives do not view IT security as a top business priority.

Infrastructure Risk

- My organization's enabling security technologies are not sufficient to protect data assets and IT infrastructure.
- My organization's IT security function does not have ability to know the physical location of business-critical data assets and applications.

Operational Risk

- My organization lacks active involvement in threat sharing with other companies and government.
- My organization's IT security function lacks security in the DevOps environment.

WHAT BUSINESSES STAND TO LOSE

While any kind of information that 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. Business communication (email)
2. Financial information
3. Analytics (data models)
4. Consumer data
5. Company-confidential information

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

Top concerns of a successful cyberattack are:

- Customer turnover
- Lost intellectual property (including trade secrets)
- Disruption or damages to critical infrastructure

THE GREATEST CYBERSECURITY CHALLENGES FOR BUSINESSES

The 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**: Many organizations stated their people aren't prepared enough to manage new attacks across employees, executives, and board members
- **Process**: Organizations lack sufficient processes to combat attacks, ranging from patching to threat sharing
- **Technology**: Organizations need to evaluate their existing security tools and ensure they're using the latest advanced detection technologies across their networks

PROTECTING BUSINESSES FROM CYBER THREATS

Taking the current threat landscape into consideration and based on the CRI findings, global businesses can still greatly 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.
- 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 BYOD, IoT and industrial IoT devices, 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.

Key takeaways for businesses

Our findings show that global businesses have a very high chance of being affected by a cyberattack:

- Likelihood of a data breach of customer data in the next 12 months: **80%**.
- Likelihood of a data breach of critical data (IP) in the next 12 months: **77%**.
- Likelihood of one or more successful cyberattacks in the next 12 months: **86%**.

TREND MICRO™

Securing Your Connected World

[EXS01_Cyber_Risk_Index_Executive_Summary_210721US]