CYBER RISK INDEX (CRI)

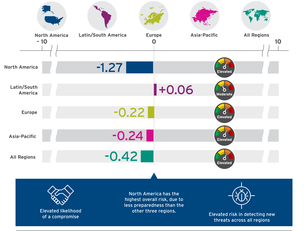
With cyberattacks a constant threat, it's crucial for companies to focus on assessing, detecting, preventing, and responding to today's cyber threats. In this iteration of the CRI, performed in 1H'2021, Trend Micro and Ponemon Institute conducted research among IT managers across Europe, Asia-Pacific, Latin/South America, and North America, using the findings to create a comprehensive index to assess an organization's cyber risk maturity level. Three of four regions showed an elevated risk level, while Latin/South America showed a moderate risk level, contributing to an overall elevated risk level worldwide.

Current global cyber risk level:

Top risk factors in the 1H'2021

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.



Elevated likelihood of a compromise

North America has the highest overall risk, due to less preparedness than the other three regions.

Elevated risk in detecting new threats across all regions

Overall

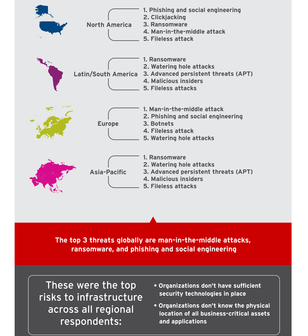
The Cyber Preparedness Index was at a moderate risk for Europe, Asia-Pacific, and Latin/South America, but North America had concerns over its ability to detect and prevent new attacks with an elevated risk level.

Overall, all organizations are at an elevated cyber risk.

All organizations show an elevated risk associated with the Cyber Threat Index, with all regions exhibiting approximately the same level of risk.

Differences Between Regions

Top 5 cyber threats



The top 3 threats globally are man-in-the-middle attacks, ransomware, and phishing and social engineering

These were the top risks to infrastructure across all regional respondents:

- **Organizations don't have sufficient security technologies in place**
- **Organizations don't know the physical location of all business-critical assets and applications**

This showcases the challenges organizations are having to deal with because of the many changes we're seeing within the infrastructure, including new cloud implementations.

Likelihood of a successful cyberattack

Across the four regions, respondents appear to be concerned they will be successfully attacked in the next 12 months. **9 of 10 in North America, Europe, and Latin/South America** and **8 of 10 in Asia-Pacific** are somewhat to very likely to be compromised in the next 12 months.

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.

North America | Latin/South America | Europe | Asia-Pacific

1 Are my organization's enabling security technologies sufficient to protect data assets and IT infrastructure? (Lower number means less prepared on 0-10 point scale)

Takeaway

With nearly **4 out of 5** 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.

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

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.

Takeaway

9 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.

Likelihood of one or more successful cyberattacks in the next 12 months:

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

Takeaway

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

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

TREND MICRO