THE 2020 CYBER RISK INDEX (CRI)

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

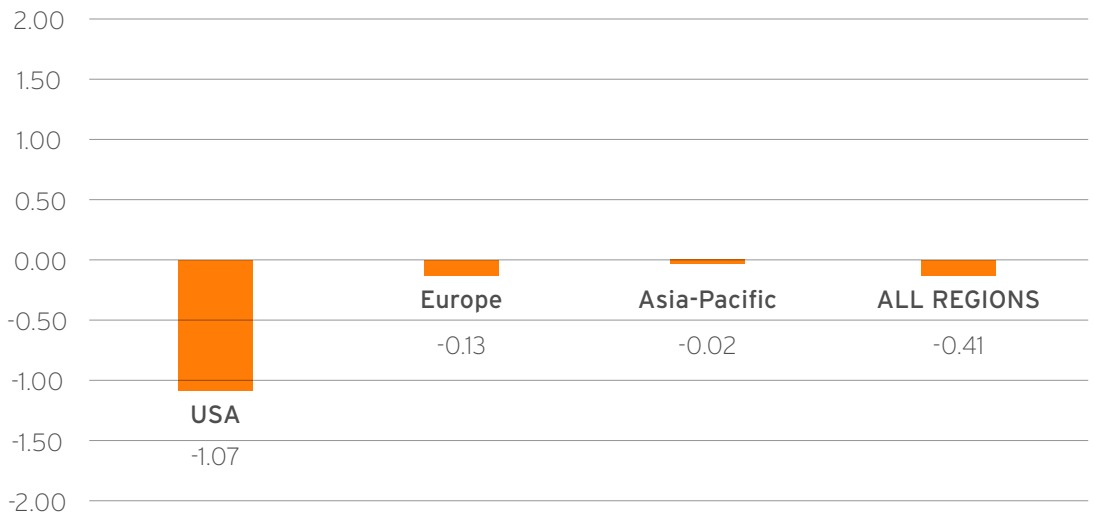
This version of the CRI was developed from a survey conducted by Ponemon Institute, which included almost 2,800 IT practitioners and managers across the USA, Europe, and Asia-Pacific.

The CRI is calculated by subtracting the Cyber Threat Index from the Cyber Preparedness Index. The scale is +10 to -10; -10 represents the highest amount of risk.

The CRI is composed of two individual indices:

- **Cyber Preparedness Index**—represents 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 2020



All regions showed an elevated risk *(negative CRI number)*, with the USA having the highest risk level compared to the other two regions. This was due to the USA having a lower perceived readiness than the other regions.

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 three regions:

Cyber Threat Risk

- Phishing and social engineering
- Clickjacking
- Ransomware
- Fileless attacks
- Botnets
- Man-in-the-middle attacks

Data Risk

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

Human Capital Risk

- My organization's senior leadership does not view security as a competitive advantage.
- My organization's IT security leader (CISO) does not have sufficient authority and resources to achieve a strong security posture.

Infrastructure Risk

- 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 function is not involved in determining the acceptable use of disruptive technologies (such as mobile, cloud, social media, IoT devices) in the workplace.

Operational Risk

- My organization is not well prepared to deal with data breaches and cybersecurity exploits.
- My organization's IT security function is slow to test and install all security patches.

WHAT BUSINESSES STAND TO LOSE

While any kind of information that a business possesses is prone to data loss or theft, these four information types are the ones that present the greatest risk for an organization, based on results from the survey.

1. Financial Information
2. Company-confidential Information
3. Consumer data
4. Business communications (email)

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: **75%**
- 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: **83%**

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:

- Lost intellectual property (including trade secrets)
- Customer turnover
- Stolen or damaged equipment
- Productivity decline

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:

- My organization's IT security function is able to contain most cyberattacks.
- My organization's IT security function has evolved over time in response to changing attacks and attack patterns (e.g, vectors).
- My organization's IT security leader (CISO) has sufficient authority and resources to achieve a strong security posture.
- My organization's enabling security technologies are sufficient to protect data assets and IT infrastructure.
- My organization spends considerable resources to recruit and retain IT security personnel.
- My organization spends considerable resources evaluating third-party security risks (including the cloud and the entire supply chain).

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

TREND MICRO™

Securing Your Connected World

Exec_Summary_2020_CRI_201118US