The 2H 2019 Cyber Risk Index (CRI)
Trend Micro, in conjunction with Ponemon Institute, presents the 2nd 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.

The Cyber Risk Index was developed from a survey of over 1000 IT practitioners and managers by Ponemon Institute.

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

The Cyber Risk Index 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.

There was a slight increase in risk (lower CRI number) since the previous CRI mainly due to survey responses indicating the threat landscape has increased the risks of new threats successfully targeting organizations.
The primary business risks

The top cybersecurity risk factors businesses face can be broken down into five categories with the top concerns from respondents:

- **Cyber Threat Risk**
  - Phishing and social engineering
  - Clickjacking
  - Botnets
  - Fileless attack
  - Denial of service (DoS)

- **Data Risk**
  - My organization's IT security function is able to detect zero-day attacks.
  - My organization's IT security function is able to prevent most cyberattacks.

- **Human Capital Risk**
  - My organization spends considerable resources to recruit and retain IT security personnel.
  - My organization spends considerable resources educating employees about security requirements.

- **Infrastructure Risk**
  - My organization’s IT security function has the ability to know the physical location of business-critical data assets and applications. My organization’s IT security function is quick to test and install all security patches.
  - My organization's IT security function is 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 well prepared to deal with data breaches and cybersecurity exploits. My organization's IT security architecture has high interoperability, scalability and agility.
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. R&D Information
2. Financial Information
3. Company-confidential Information
4. Customer Accounts

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

Top concerns of a successful cyberattack are:

- Disruption or damages to critical infrastructure
- Stolen or damaged equipment
- Cost of outside consultants and experts
- 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 survey results, these are the greatest preparedness areas of concern for businesses:

- My organization is well prepared to deal with data breaches and cybersecurity exploits.
- My organization’s IT security function is able to detect zero-day attacks.
- My organization’s IT security function is able to prevent most cyberattacks.
- My organization is actively involved in threat sharing with other companies and government.
- My organization’s IT security function has the ability to know the physical location of business-critical data assets and applications.

Key takeaways for businesses

Our findings show that 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: 78%
- 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: 81%
Protecting businesses from cyber threats

Taking the current threat landscape into consideration, our findings based on the CRI show that 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™ RESEARCH
Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com