With cyber attacks a constant threat, it's crucial for companies to focus on assessing, detecting, preventing, and responding to today's cyber threats. In its second iteration of the CRI performed in 2H'19 Trend Micro and the Ponemon Institute conducted research among IT managers, using the findings to create a comprehensive index to assess an organization's cyber risk maturity level. The cyber risk increased since the last time mainly due to an increase in the range of exploitable vulnerabilities, including those targeting critical infrastructure and critical business data.

Key business risks:
- Data breaches
- Productivity decline
- Cost of outside consultants and experts
- Equipment damage or theft
- Stolen or damaged business-critical data
- Breach of critical data
- Business-interruption insurance claims

The top four data types at highest risk of loss or theft are:
- Customer accounts
- Company-confidential business-insurance policies
- Customer-privileged personal information
- Internal accounts

The difference in risk level by industry:
- Health & Pharma
- Banking/Mfg
- Public Sector
- Financial Services
- Hospitality
- Industrial/Construction
- Automotive
- Retail
- Media/Entertainment
- Others

Takeaways:
- The average CRI across all organizations increased by 4.61 from 2H'18 to 2H'19.
- Small Business has a lower CRI indicating it is a lower risk than Medium Business, which is lower than Enterprise.
- The Cyber Risk Index results across multiple industries shows nearly all industries have a higher CRI in 2H'19 compared to 2H'18.
- Cyber-attack reporting is increasing, with 21% of organizations experiencing 4+ attacks in 2019 compared to 15% in 2018.
- The percentage of organizations that had >10 breaches in the last 12 months increased from 69% to 73%.
- The percentage of IT leaders who are very prepared to deal with an attack has decreased from 77% to 69%.