# 5th Seminar on Current Issues in General Insurance

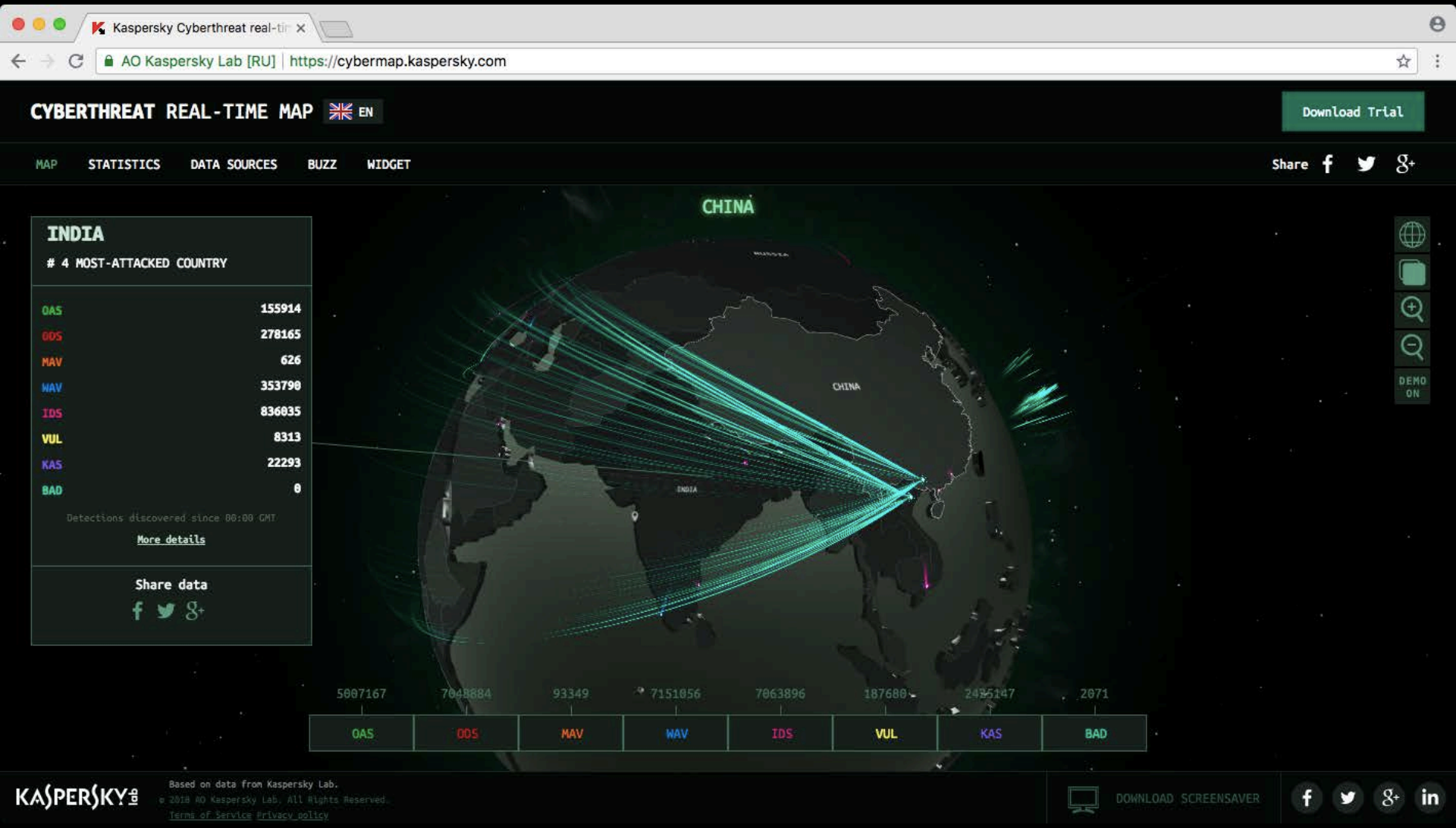
# Cyber Risks and Insurance Solutions

**Shashank Bajpai**
**Chief Information Security Officer at ACKO**

Institute of Actuaries of India

# Cyber Threat > IT Risk

- Hackers/Fraudsters are just next door
- No State Boundary
- Local Incident – Global Effect
- State Sponsored Cyber Attacks
- Data Breach vs Privacy Breach

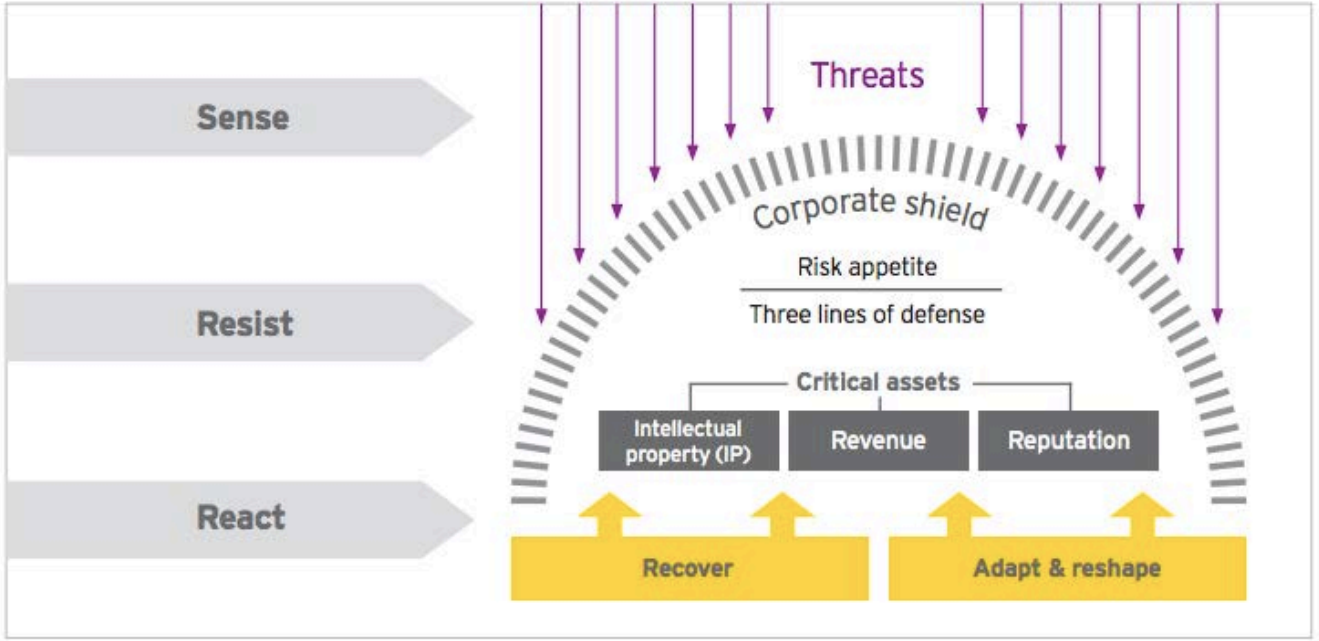

Kaspersky Cyberthreat real-tir
AO Kaspersky Lab [RU] | https://cybermap.kaspersky.com
CYBERTHREAT REAL-TIME MAP
EN
Download Trial
MAP
STATISTICS
DATA SOURCES
BUZZ
WIDGET
Share
INDIA
# 4 MOST-ATTACKED COUNTRY
OAS 155914
DOS 278165
MAV 626
WAV 353790
IDS 836035
VUL 8313
KAS 22293
BAD 0
Detections discovered since 00:00 GMT
More details
Share data
CHINA
INDIA
DEMO ON
5007167
7048884
93349
7151056
7063896
187680
2435147
2071
OAS
DOS
MAV
WAV
IDS
VUL
KAS
BAD
KASPERSKY
Based on data from Kaspersky Lab.
© 2018 AO Kaspersky Lab. All Rights Reserved.
Terms of Service Privacy policy
DOWNLOAD SCREENSAVER

# Cyber Risk – The Definition

- Any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or services. The impairment of operational technology (OT) eventually leads to business disruption, (critical) infrastructure breakdown, and physical damage to humans and property.
- Cyber risk is either caused naturally or is man-made, where the latter can emerge from human failure, cyber criminality (e.g. extortion, fraud), cyberwar, and cyber terrorism. It is characterised by interdependencies, potential extreme events, high uncertainty with respect to data and modelling approach, and risk of change.

# Cyber Risk – Status Quo

- In spite of its increasing relevance for businesses today, research on cyber risk & related insurance is limited.
- Focus has always been on the technological aspects, but relatively very less efforts have been put from a business and economics aspect.



# Cyber Risk – Status Quo

- There are special standards and tools for cyber risk management. In each step of the classical risk management process, cyber risks show special features.
- Institutional commitment, effective crisis management, risk communication with employees, customers and suppliers, and continuous monitoring are fundamental.
- Cyber risk management today focuses on risk mitigation, while risk transfer so far plays only a minor role.


INSURANCE

# Cyber Insurance – Status Quo

- The cyber insurance market is very small at present compared to other lines of business, but is expected to increase significantly in the coming years. The U.S. is far ahead of Europe and Asia, for example, with regard to reporting requirements.
- The main insurability problems are the lack of data, risk of change, accumulation risk, and potential moral hazard problems.

# Contd…

- There is a **stunning gap** between the nature of new threats and the capabilities available to detect attacks, monitor (and stop) unauthorized exfiltration, and secure information.
- Many Insurers do not have the tools to provide the direct **real-time** awareness necessary to calculate risks to insured digital assets stored by cloud service providers or enterprise networks.
- There is **increased awareness** that companies should be accountable for private records and the security of data collected from their customers.
- Insurers should make the fundamental **assumption** that any insured infrastructure will at some point be compromised, if not already.

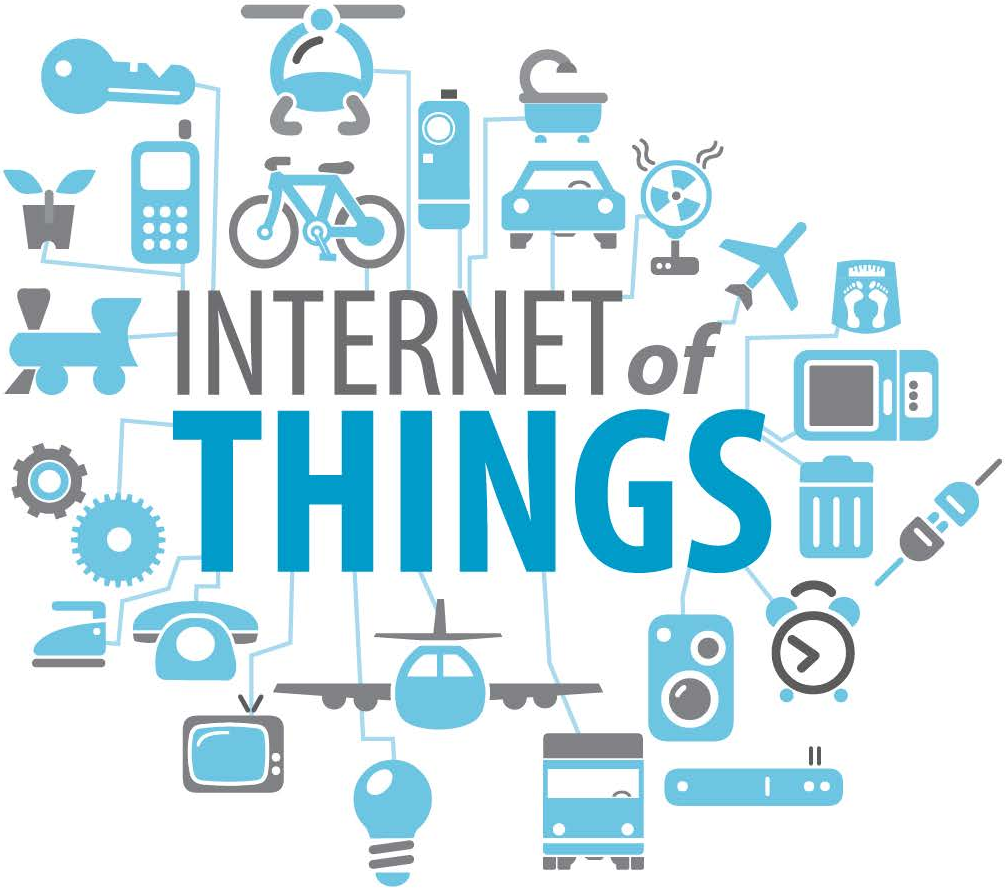
# Existing Insurance Solutions for Cyber Risk

- Coverage of Cyber Insurance Solutions **vs** Damage done by Cyber Attack
- Measuring the **Reputational Loss** by a Cyber Attack
- Digital Business **vs** Offline Business
- Challenges in detecting **Fraudulent Cyber Claims** and ascertaining the damages resulting from a State Sponsored Cyber Attack
- Its just not “Who” or “What” we have to Insure…. Its now “**When**” we are Insuring Cyber Risk - Timestamp
- In a Digital Connected World – it is still very opaque and Black & White for Cyber insurance .. Why (ecommerce example)


BLOCK CHAIN
TECHNOLOGY

# Cyber Risk & Insurance – What lies ahead

- To prevent cyber risks: develop standards, common language, and good practices; conduct scenario analysis; initiate and/or intensify dialogue with stakeholders; track technological development (cloud computing, Internet of Things(IoT), blockchain technology etc.), increase own analytical skills (digital forensic) and make own IT more resilient.
- To support cyber insurance: develop anonymised data pools, develop (re-)insurance pools, analyse existing policies and develop new ones


INTERNET of
THINGS

# Cyber Risk & Insurance – What lies ahead

- IOT a new dimension of Cyber Risk–
  - Smart Mobility
  - Smart City
  - Smart Manufacturing
  - Smart Life
- New methods are needed to definitely identify the cause of cyber-compromise, the assets affected, time exactly “when” the compromise occurred, and if insured assets were directly/indirectly exposed outside the organization.

Institute of Actuaries of India

# THANK YOU !!!

# References

- https://goo.gl/GwzMLV
- https://goo.gl/b4TBvn
- https://goo.gl/URJ6uY
- https://goo.gl/Dahhqq
- https://goo.gl/ZMQxaG