



**ASIA-PACIFIC TELECOMMUNITY**

**5th APT CYBERSECURITY FORUM (CSF-5)**

26-28 May 2014, Ulaanbaatar, Mongolia

**Document  
CSF-5/INP-19**

24 May 2014

---

**Mr. CHINZORIG GANBOLD, ITPTA,  
(Mongolia)**

**CYBERSECURITY POLICY IN MONGOLIA**

---

**Contact :**

Mr. CHINZORIG GANBOLD ,  
ITPTA, Mongolia

Tel: +976-89119800  
Email: [Chinzorig@itpta.gov.mn](mailto:Chinzorig@itpta.gov.mn)



GOVERNMENT OF MONGOLIA  
INFORMATION TECHNOLOGY, POST  
AND TELECOMMUNICATIONS AUTHORITY  
[WWW.ICT.MN](http://WWW.ICT.MN)

# Cyber security policy in Mongolia

Chinzorig Ganbold  
Director of IT & Innovation division  
ITPTA

# Agenda

- National program for Information Security
- Challenges in implementing National program
- Emerging issues
- Conclusion





GOVERNMENT OF MONGOLIA  
INFORMATION TECHNOLOGY, POST  
AND TELECOMMUNICATIONS AUTHORITY  
[WWW.ICT.MN](http://WWW.ICT.MN)

# **NATIONAL PROGRAMME FOR INFORMATION SECURITY**

# Parties responsible for National program implementation



PRIME MINISTER  
OF MONGOLIA



Information  
Technology Post and  
Telecommunication  
Authority (ITPTA)



Cyber Security  
Department



# Structure of programme

- Objectives
  - Establishing legal framework for information security
  - Mitigating information security risks and building a structure to handle incident response
  - Maturity ICT usage culture, raising public awareness and knowledge about IS, HR development, and developing public private partnership
  - Establishing information security framework for government
- Duration
  - 2010 -> 2015



# Principles of National programme

- 2.2.1. Compliant with National security guidance and laws;
- 2.2.2. Adopting international trends and standards
- 2.2.3. Promoting public-private partnership and public involvement, and strengthening the coherence between these stakeholders
- 2.2.4. Protecting the critical infrastructure both by the government and the private sector;
- 2.2.5. Implementing the program guided by Risk Assessment
- 2.2.6. Fostering the international cooperation in a transparent manner
- 2.2.7. Protecting privacy and human rights



# Legal framework

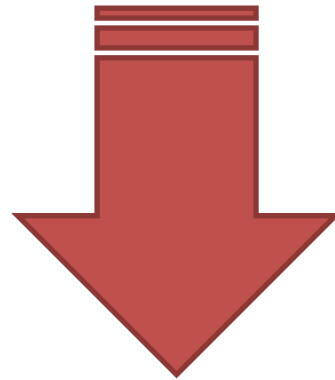
- Developed draft of Cyber security law
- Cabinet decree No.312
- Adopted international standards
  - ISO/IEC 2700x (5 standards)
  - MNS ISO/IES 13335-1:2009
  - MNS ISO/IES 17799:2007
  - MNS 5969:2009 IT & information security techniques and risk management





# Risk management

- First-ever government-wide risk assessment on Information security
  - First quarter of 2013
  - 22 government entities who run significant IT systems were assessed (out of 85)
  - Assessed on 8 different criteria

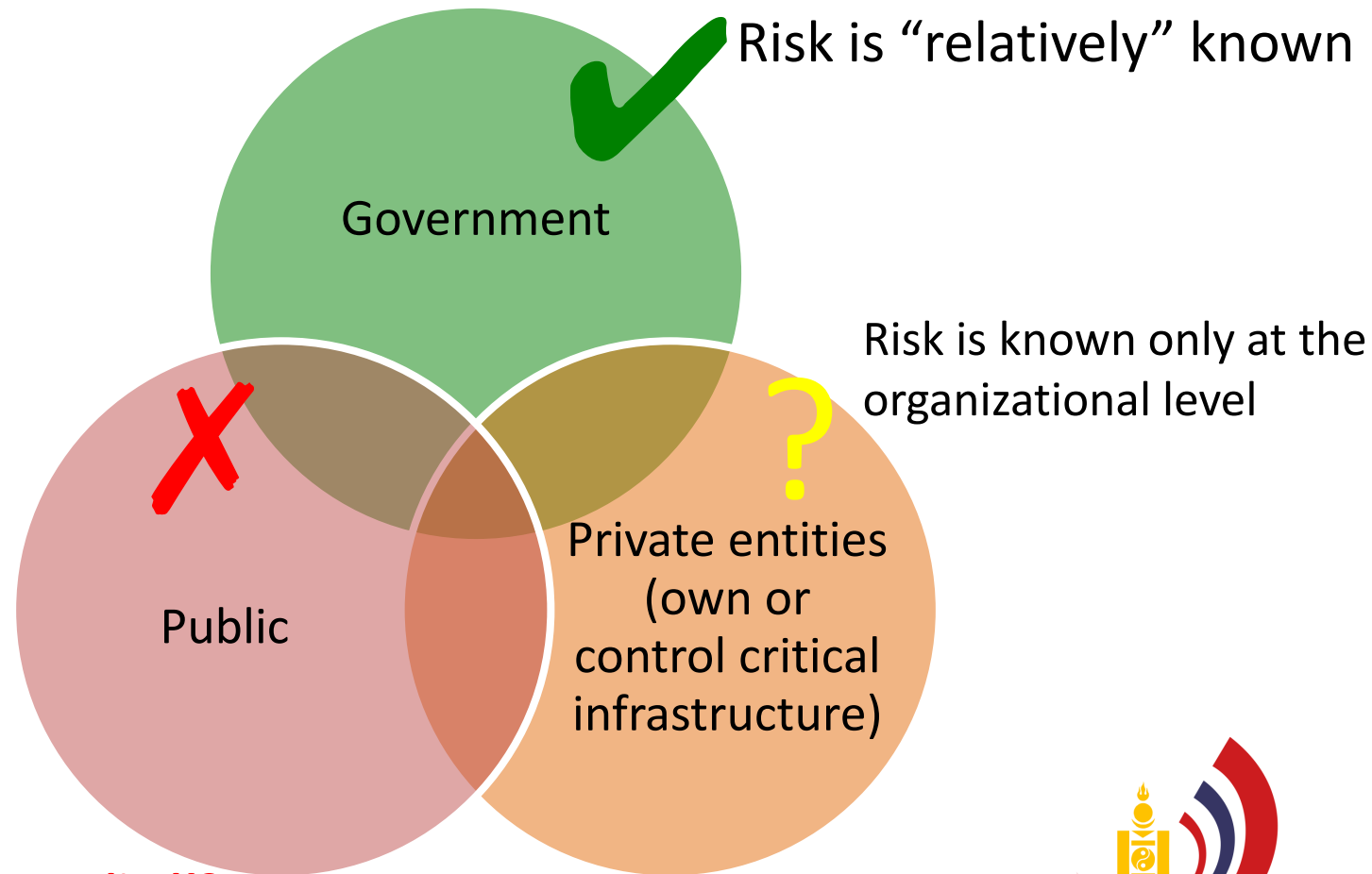


**Now, we know the level of risk  
on a government level!**

**But...**



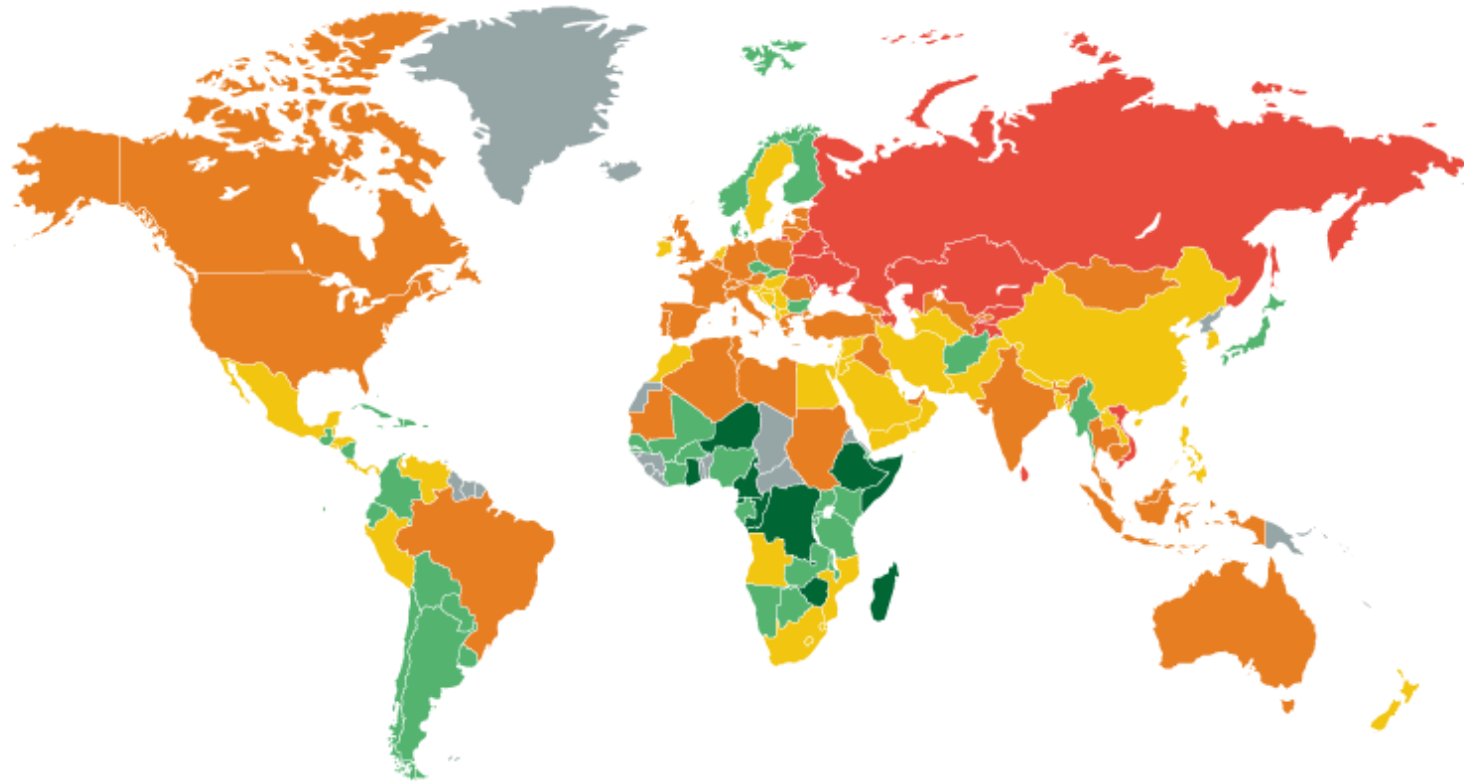
# Cyber security risk for stakeholders



**Risk was never studied!?**



# Risk of computer infection via Internet



Infection %

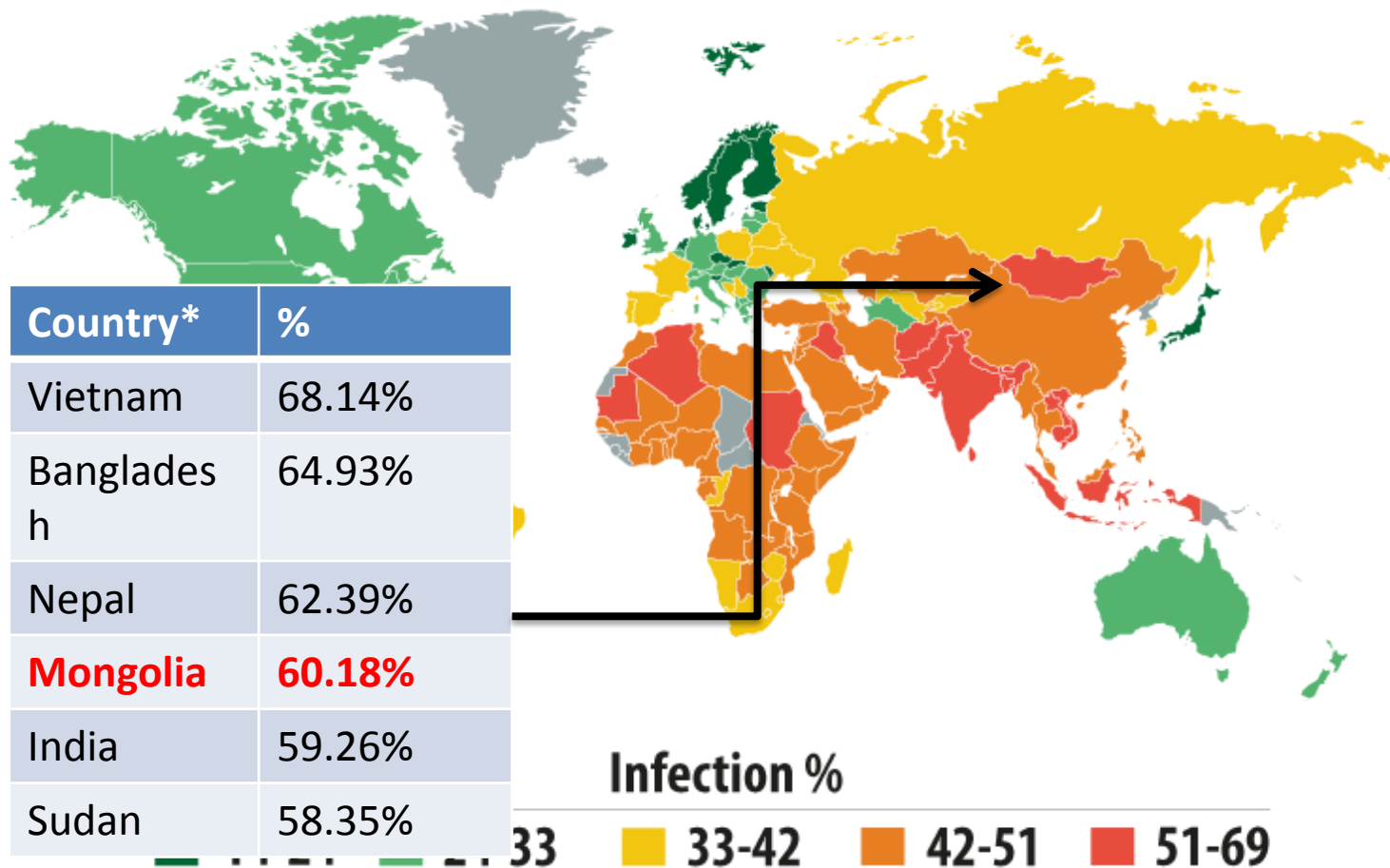


Kaspersky Security Bulletin 2013



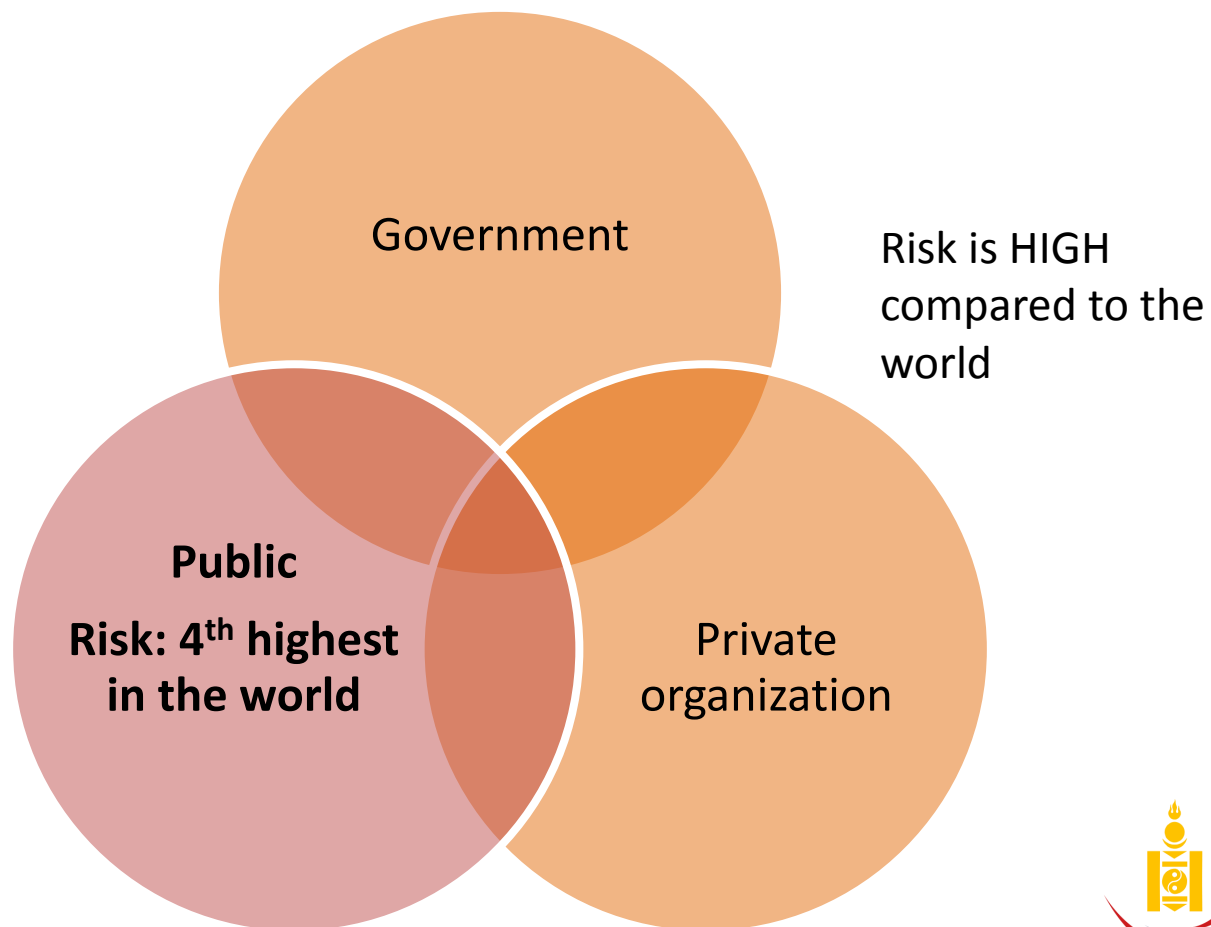
# Risk of local infection

Reflects the level of personal computer infections



Kaspersky Security Bulletin 2013

# Cyber security risk of stakeholders





GOVERNMENT OF MONGOLIA  
INFORMATION TECHNOLOGY, POST  
AND TELECOMMUNICATIONS AUTHORITY  
[WWW.ICT.MN](http://WWW.ICT.MN)

# **CHALLENGES IN IMPLEMENTING THE NATIONAL PROGRAM**

# Lack of public awareness

**Local infection risk: 4<sup>th</sup> highest in the world**



- Public at large ignores the cyber threats by believing such threats only apply to businesses, not individuals



# Obscurity of attacks and threats

- Critical infrastructures
    - Banks
    - Telco operators
    - Others
- Information is not shared

**“Yet security through obscurity is not a viable defense model against modern cyber threats.” ... *ITU Global Cybersecurity Index Conceptual Framework***





# Scarce resources

- People - Too few experts
  - One state organization = Cyber Security Department
  - Lack of competition between security consulting companies
  - Absence of domestic security vendor
- Budget – dispersed funding





GOVERNMENT OF MONGOLIA  
INFORMATION TECHNOLOGY, POST  
AND TELECOMMUNICATIONS AUTHORITY  
[WWW.ICT.MN](http://WWW.ICT.MN)

# EMERGING ISSUES

# Emerging issues

- Recent news headlines
  - China Suspends Cyber Security Cooperation with US
  - Cisco CEO Tells Obama That NSA-Installed Backdoors are Not Good for the Economy



**Now, who is the good guy?**



# Emerging issues -> Response

- Mongolia needs its own Cyber Security Evaluation Center
  - Security clearance for every network device imported

## Examples:

- Huawei funded Cyber Security Evaluation Center of UK where the UK tests Huawei gear to make sure there are no backdoors installed
- Chinese DDoS mitigation vendor NSFocus pays US application security test company Veracode to do the same for their products



# Conclusion

- “Although cybersecurity efforts are numerous, they are eclectic and dispersed.” ... *Global Cybersecurity Index Conceptual Framework*



- We need cooperation at all levels
  - Locally and globally
    - Information and knowledge is shared
- Mongolia needs to actively reverse the bottom-up approach to top-down for cybersecurity

**WE NEED TO BE PROACTIVE!**





GOVERNMENT OF MONGOLIA  
INFORMATION TECHNOLOGY, POST  
AND TELECOMMUNICATIONS AUTHORITY  
[WWW.ICT.MN](http://WWW.ICT.MN)

**Thank you for your attention**