Organizer:

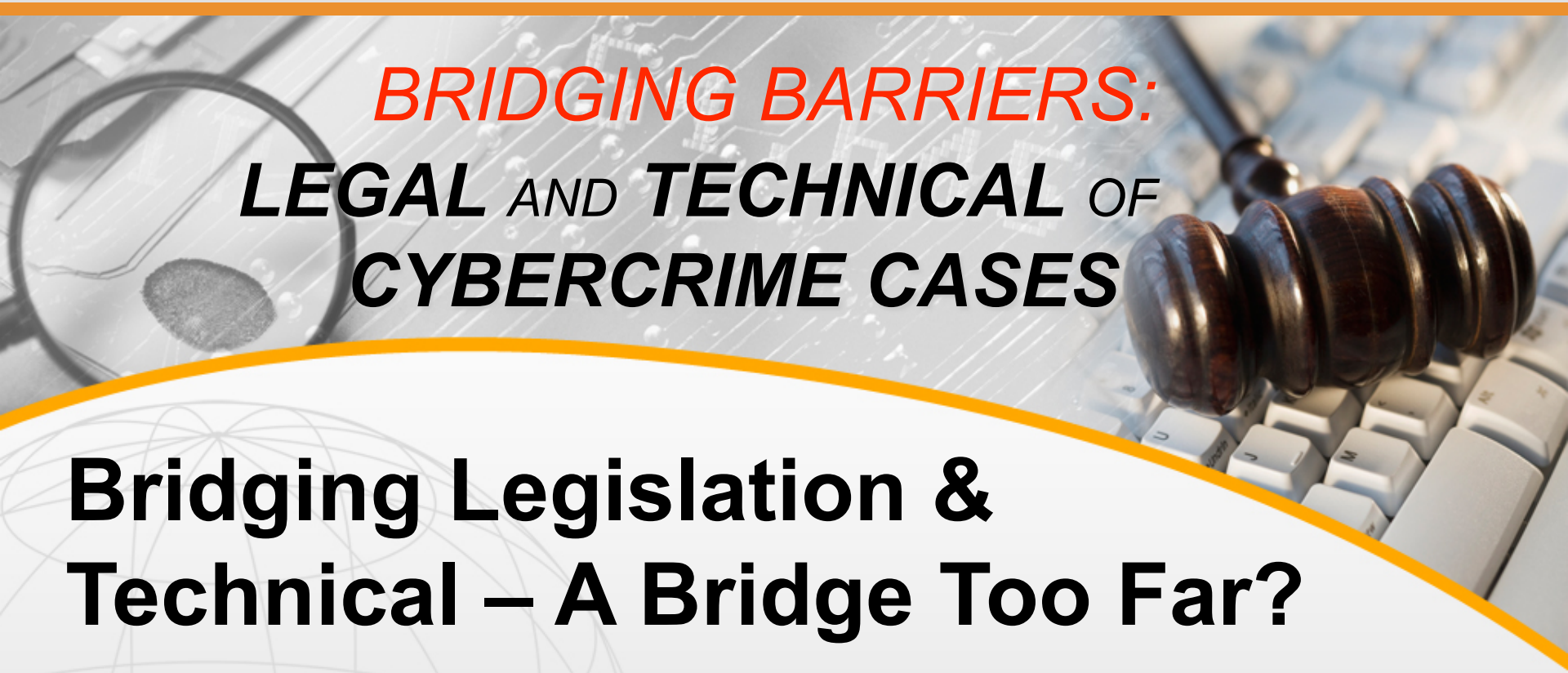
CyberSecurity MALAYSIA

AGCSM

Endorsed by:

People First, Performance Now

MOSTI Ministry od Science, Technology and Innovation



BRIDGING BARRIERS: LEGAL AND TECHNICAL OF CYBERCRIME CASES

Bridging Legislation & Technical – A Bridge Too Far?

Harme Mohamed

Malaysian Communications and Multimedia Commission

7 July 2011

Penetration Rates

Broadband

60.1%

(per 100 households)

Celullar

121.0%

(per 100 population)

Fixed

42.6%

(per 100 households)

Television

Peninsular: 96%

Sabah & Sarawak : 88.4%

Radio

Peninsular: 94.9%

Sabah & Sarawak : 88.1%

Relevant Legislation

- Penal Code
- Criminal Procedure Code
- Sedition Act 1948
- Evidence Act 1950
- Dangerous Drugs Act 1952
- Copyright Act 1987
- Banking and Financial Institutions Act 1989
- Extradition Act 1992
- Computer Crimes Act 1997
- Communications and Multimedia Act 1998
- Mutual Assistance in Criminal Matters Act 2002

ANATOMY OF CYBERCRIME

Cybercrime

- Crimes performed in and with computers, computer networks and increasing mobile communications (smart phones)
- Computers, and data stored in them are:
  - Targets (hacking, DDoS-attacks, defacements, etc.)
  - Tools (host and create undesirable content, fraud, forgery, originate attacks, etc.)
  - Device that contains evidence of crimes (drug trades, terrorism)
- International, not bound by territorial borders

Investigation

- Investigation and analysis of ‘hardcore’ cybercrimes, such as botnets, hacking and malwares
- Investigation and analysis of the role and use of computers in the combat against crime in general, such as frauds and undesirable contents
- No single crime scene to process and combination of attacks to be analyzed
- Changing requirements of an Investigating Officer
- Requires new methods of surveillance and investigations

Evidence Gathering

- Sometimes still need tried and tested methods
- The discipline is very much the same, statement taking etc. but need to know what to ask etc. (criminal conduct and exploited technology)
- Importance of analysis & forensics capabilities
- Usage of appropriate tools which are available

CHALLENGES

Key Considerations

- Balance between the privacy of citizens and effectiveness of law enforcement
  - Preventive measure – put in technological infrastructure to combat cybercrime
- Classification of techniques (social engineering, malware, network breaches) – are the current laws able to identify and deal with these techniques?
- International cooperation
- Anti-forensic tools and anonymization technologies

CONCLUSION

Conclusion

- Existing laws need to be reviewed to keep abreast of new technologies but not to stifle innovation of new technologies and services
- Need clear process and procedures and empowerment to law enforcement agencies
- Need to encourage home-grown technologies to assist investigations and evidence gathering