Regional Cybercrime-Cybersecurity Assessment Conference

Manila, Philippines, 11–12 November 2015

Statistics and Reporting Mechanisms

Discussion template

Please complete this template as far as possible before attending the workshop and bring it with you for reference during the interactive sessions. You may then complete it during the workshop.

Country:	

Part 1: Statistics on cybercrime and electronic evidence

1. What is the purpose/benefit of collecting statistics on cybercrime and cases involving electronic evidence?

2. What systems or mechanisms exist to record police and criminal justice statistics in your country? Please provide a short summary, if possible with links to relevant documents or websites.

3. Do such statistics specifically distinguish cases of cybercrime and cases involving electronic evidence? If so, according to what classification?

4. Do your authorities prepare regular threat assessments on cybercrime, organised crime or other types of crime? If so, please provide a short summary, if possible with links to relevant documents or websites.

5. How are cases involving electronic evidence identified and recorded?

6. Who collates and who analyses the statistics?

7. What are analyses of cybercrime statistics used for?

8. From your national statistics databases would it be possible to answer these questions?

	YES	NO
• How many phishing reports were made nationally?	☐	☐
• What was the median loss from cyber-fraud?	☐	☐
• How many reports of Advance Fee Fraud were made nationally?	☐	☐
• How many cases of cyber stalking were reported in your capital city?	☐	☐
• How many cases involved a female victim?	☐	☐
• How many cases involved a victim under the age of 14?	☐	☐
• How many cases involved evidence from an electronic device?	☐	☐

- How many cases involved evidence referred for digital forensic examination? ☐ ☐
- How many cases involved potential evidence from an electronic device that was not referred for digital forensic examination? ☐ ☐
- How many cases of cybercrime or electronic evidence involved sending a Rogatory Letter? ☐ ☐

Part 2: Cybercrime reporting systems

9. What systems/mechanisms currently exist for the general public to report cybercrime? (check all boxes that apply)

- In person to a police officer ☐
- By letter ☐
- By telephone ☐
- By email ☐
- By online reporting site ☐
- To an agency other than a law enforcement body ☐

10. Which agencies or authorities accept reports of cybercrime?

11. If you have an online reporting system, please provide a short summary of how it functions and a link

12. What are the criteria for classifying a report as cybercrime?

	YES	NO
13. Are the same criteria used by all agencies that accept reports?	☐	☐
14. Is there an agreed common reporting template used by all agencies?	☐	☐

15. How is the cybercrime report documented and processed by the reporting agency?

- On paper in hard copy only ☐
- On paper and then transferred to a computer database ☐
- Electronically by a law enforcement officer ☐
- Automatically online by the member of the public ☐

16. Which Authority is responsible for collating cybercrime reports into national statistics?

	YES	NO
17. Does that Authority receive all reports from all the different reporting agencies?	☐	☐

18. How are cybercrime reports assigned for investigation?

19. Is the private sector involved in reporting cybercrime activity? If so, how?

20. In conclusion: what are your proposals regarding improving/developing i) the collection of cybercrime and cases involving electronic evidence statistics and ii) cybercrime reporting systems in your country? What steps should be undertaken?