**Lesson 3.x Skills building in cybercrime**

|  |  |  |
| --- | --- | --- |
| Lesson 3.x Skills building in cybercrime | | Duration: 130 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Internet access (if available) * PowerPoint or other presentation software | | |
| **Session Aim:**  The aim of this session is to check level of delegates understanding of previously presented topics through practical case study analysis. | | |
| **Objectives:**   * *To analyse case study synopsis in the group work environment* * *To apply knowledge acquired during the Basic Judicial Training on Cybercrime and Electronic Evidence in the case study* * *To report about case study conclusions* * *To understand what the next steps should be for developing knowledge and skills regarding cybercrime* | | |
| **Trainer Guidance**  During the session following topics should be considered:   * Introduction to the case study * Group division * Allocation of the time for the analysis * Allocation of the time for the Group Reporting * Case study * Group reporting * Questions addressing * Conclusions of the exercise | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The opening slides are the introduction to the session and include the Agenda and the session objectives. | |
| 4 to 7 | These slides are presenting the introduction to the exercise itself with short explanations about logistical arrangements for it.  Case study is envisaged to be a modular one, meaning that different setups of the exercise can be organized. Case study is modular in the way that one, two, four or different number of the groups can work on it, depending on conditions. Every group, when more than one, will get its part of the case story and it will prepare its part of the case report.  Ideally, four groups should be formed, and each group should get its part of the Study. Group 1 should be working on “Who I am?” slides, Group 2 should be working on “Follow the Data” slides, Group 3 should be working on “Follow the Money” slides, while Group 4 should be working on “Follow the Leader” slides. If the delegate numbers are different, expert should adapt this division.  On the end, all groups while reporting will actually merge partial reports to one big and final, realizing that all of them worked on one case and participated in making one story board while resolving the case with joint conclusions.  Depending on the local training conditions expert should make necessary adjustments with delegates. Detailed Case Study synopsis is available as additional training material.  For on-line version of the training, case study can be organized in the way that delegates are belonging to one group while expert is leading them through the facts, questions, and solutions, while actively engaging with them. | |
| 8 to 18 | These slides are presenting Case Study Scenario.  Case study is deriving form one of the actual and still on-going cases in one of the Cybercrime Convention parties. It represents study of the new ways of how money laundering can be organized by the abuse of the social media, on-line payments systems and on-line betting systems.  However, in its’ core this case includes already familiar definitions and terms of illegal access, data interference, computer-related forgery, computer-related fraud, offence related to infringements of copyright and related rights on the substantive law side.  On the procedural side, tools like expedited preservation and partial disclosure of traffic data, production order, search and seizure of stored computer data, real-time collection of traffic data and interception of content data are used.  Mutual legal assistance part is using extradition, expedited preservation and partial disclosure of traffic data, expedited disclosure of preserved traffic data, mutual assistance regarding accessing of stored computer data, mutual assistance regarding the real-time collection of traffic data, mutual assistance regarding the interception of content data and 24/7 network articles of the Budapest Convention | |
| 19 to 21 | These slides are presenting tasks, issues and possible questions about the case study.  Expert should present main issues which represent basically main ideas about the case which should be explored during the group work time.  Main questions are covering all chapters of the Cybercrime Convention. Conclusions should be focused on the criminal acts and procedural and MLA provisions used for the case analysis.  Case is not ready for the Court. | |
| 22 | This slide represents Group 1 specific questions and answers regarding the case study.  Answers:   * if no retention regime, Article 16 followed by Article 18. If retention in place, Article 18 to the Social Media Network regarding content data. Contact with Brand HQ about the game; * if no retention regime, Article 16 followed by Article 18. If retention in place, Article 18 to the Social Media Network regarding basic subscriber information; * witness hearing and bank account checks; * Article 8; * identification of the persons administrating the prize-winning pages and their interrogation. | |
| 23 | This slide represents Group 2 specific questions and answers regarding the case study.  Answers:   * if no retention regime, Article 16 followed by Article 18. If retention in place, Article 18 to the ISP regarding basic subscriber information, traffic and content data; * IP addresses used by administrator of the channels, administration activity logs, user activity logs regarding personal data exchange, other evidence regarding money flow and communication; * IP addresses obtained under Articles 16 and 18 will be connected to the ISP subscribers and their subscriber contracts; * Article 19 on the computers in suspects possession, suspects interrogation, Brand, Bank, Social Media, ISP representatives' statements and acquisition of additional data connected to the previous, identification of the host service provider for Dark Market in Country A, depending on the path delegates take about Dark Market provider (is its existence known to the provider or not), Articles 16, 18 and 19, log analysis of the exchange between sellers and buyers of the personal data and additional evidence with that regards. Articles 20 and 21 can be used for data collection and data interception between private data sellers and buyers providing that their IP addresses are identified; * Article 19 implementation on the suspects computers showed presence of the controller for the trojan malware installed on some Brand computers enabling access to the original channels; * by the electronic evidence acquired through use of Article 19 on the private data sellers and buyers' computers which will show bank records and cryptocurrency wallet; * Articles 2 and 4 for accessing and alteration of the original Brand social media channels, Article 7 and 10 regarding abuse of the prize-winning game in behalf of the Brand and use of the Brands logo and other IPR elements | |
| 24 | This slide represents Group 3 specific questions and answers regarding the case study.  Answers:   * logging credentials and money transactions; * yes, on-line payment company (OLPC) in Country B endorses voluntary cooperation thus request for it should be sent by Country A authorities in accordance with company rules; * Article 29 and 31 for OLPC regarding user accounts, Article 30 regarding data about communication with Country C on-line betting company (OLBC) * Articles 29 and 31 should be prepared for the Country C as well since it does not endorse voluntary cooperation, while Article 26 can be used for the fast exchange of the information between LEAs’ * Country A, B and C can organize together implementation of the Articles 33 and 34 between Country A users of the Country B OLPC and Country OLBC accounts | |
| 25 | This slide represents Group 4 specific questions and answers regarding the case study.  Answers:   * OLPC account owner and use, transaction logs, IP logs regarding communication with OLBC accounts, IP logs about communication with Country A banks, Articles 29, 30 and 31 regarding previous data flow and exchange; * yes, since OLPC is endorsing voluntary cooperation, so before Articles implementation BSI and some traffic data can be sought; * Country A will now focus on persons who are receiving payments on their Bank accounts; * Country A now comes back to Article 16, 18 and 19 regarding ordering of the money transfers from OLPC to the local banks, and if needed Articles 20 and 21 can be used for traffic and content data between main culprits and money mules; * for the Social Media Articles 16 and 18 for the re-check on previous BSI, for the VOIP Articles 20 and 21; * Case Study has open ending, Article 26 should be used and if delegates want to ask for arrest of the main suspect in Country E and extradition Article 24 can be used. | |
| 28 to 31 | Slides which are introducing and following group reporting. | |
| 31 to 33s | The final slides allow the trainer to review the learning objectives with the audience so that they may be sure that they have been achieved. It is also an opportunity for the delegates to raise any issues that may be outstanding or where they have not fully understood the subjects presented.  In addition, the trainer may use the session to check the knowledge learned by asking questions of the participants. This is important as there is no formal assessment for the course. | |
| **Practical Exercises**  Case study is envisaged in this lesson. | | |
| **Assessment/Knowledge Check**  No knowledge check or assessment has been requested for this session. | | |