Appendix J

Cybercafe Due Diligence Questionnaire

Introduction

The context for this appendix comes from the discussion in Section 2.5 in Chapter 2. Netizens accessing Internet at Cybercafe can be categorized under two groups. The term “Netizen”’ is introduced in Section 1.10 in Chapter 1. “Netizen” is someone who spends considerable time online and also has a considerable presence online through websites about the person, through his/her active blog contribution and/or also his/her participation in the online chat rooms. The first category of netizens are the users who do not have computer with Internet connection at their home, and therefore they visit cybercafes more frequently (i.e., 3 to 4 times a week). The second category of netizens seldom visit cybercafe; they only visit cybercafe when they have some problem with Internet connection at their home or when something goes wrong with their computer. (Box J.1 explains new category of netizens.)

Box J.1: Net Cafe Refugees/Cyberhomeless

Net cafe refugees are also known as cyberhomeless. The terminology is used for growing class of homeless people in Japan who do not have own permanent residence and/or cannot afford an accommodation on rent. They live, sleep and stay in the cybercafes that are available for 24 hours. Such cybercafes originally provided only Internet services and subsequently started offering food, drinks and showers. The objective behind providing this facility is for the commuters who miss the last train; however, the net cafe refugee trend has seen large numbers of people use it as their home.

Source: http://en.wikipedia.org/wiki/Net_cafe_refugee (10 January 2011).

Cybercafes become a medium for many cybercrimes because of security flaws exploited by the hackers while operating from cybercafe. Cybercafe users who are not IT savvy and/or the users who visit occasionally will not be able to know what applications are installed on the computer systems. As a result, there is extremely real threat from malicious programs such as key loggers or Spyware (explained in Section 4.5 in Chapter 4) with the aim to capture the keystrokes to obtain the User IDs as well as passwords along with other private information or check the browsing activities.

This appendix can be used to find the status of DUE DILIGENCE at the visited cybercafe to understand awareness about cybersecurity among cybercafe operators as well as to know the established cybersecurity measures with the help of the checklist presented in Table J.1.

Table J.1 Cybercafe due diligence questionnaire

Sr. No.	*Cybercafe Details*
1	Name of the cybercafe:
2	Postal address:
3	Name of the owner:
4	Cybercafe commence on (Mon/YYYY) :

5	Whether cybercafe is registered with CCAOI (Cyber Café Association in India):
6	Total no. of computers:
7	Total computers in working condition:
8	Name of the ISP (Internet Service Provider):
Sr. No.	***Questions***
9	Who operates the cybercafe (owner or contractors)? • If operated by contactors, is the contract registered under court of law? • Is the contractor aware about all the clauses mentioned under the contract?
10	Has the cybercafe operator undergone any training related with cybersecurity before/after cybercafe has commenced? (If yes, capture the details mentioned below.) • Training Institute and Training Course: • Name of the Institute: • Name of the Course: • Duration of the Course:
11	Is any computer software used to monitor the cybercafe operations and users? (If yes, capture the details mentioned below.) • Name of the computer software: • Name of the vendor/distributor: (from where the computer software has been purchased)
12	Do you maintain the record of each and every cybercafe users? (If yes, capture the details mentioned below.) • How is the record maintained? (Through automated system/in the spreadsheet/in the register). • Name of the user: • Cell no.: • Start Time: • End Time: • Identity proof details:
13	Do you have the AMC (Annual Maintenance Contract) for computer software mentioned under Sr. No. 11 to obtain any required support? (If yes, capture the details mentioned below.) • Name of the agency: • AMC Period: • Validity of AMC:
14	Do you have the AMC (Annual Maintenance Contract) for computer hardware and spare-parts to obtain any required support? (If yes, capture the details mentioned below.) • Name of the agency: • AMC period: • Validity of AMC: • Type of the contract (comprehensive/non-comprehensive):
15	Is antivirus software installed on each computer system? (If yes, capture the details mentioned below.) • Name of the antivirus: • Version no.: • Name of the vendor/distributor: (from where the antivirus software has been purchased)

16 Does each computer system have the latest antivirus software version installed on it?

- Does it contain the latest updated virus signatures as per vendor release?
- Are all the patches released by the vendor installed on all the computer system?

17 Is IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) installed on the main server? (If yes, capture the details mentioned below.)

- Name of the IDS/IPS:
- Version no.:
- Name of the vendor/distributor:
  (from where the IDS/IPS has been purchased)
- Are all the patches released by the vendor installed on all the computer system?

18 Do you have "Software Licenses Contact" in place for the all softwares installed at cybercafe? (If yes, check and verify licenses for each computer software installed on each machine as mentioned below.)

- OS (Operating System):
- Office automation software (e.g., Microsoft Office):
- Antivirus software:
- IDS/IPS:
- Cybercafe monitoring software:

19

- Do you regularly (quarterly/six monthly/annually) format the hard disk of each computer system at the cybercafe?
- Do you maintain the record for this activity for each computer system at cybercafe?

20 Is the access forbidden to the adult websites (e.g., pornographic websites)? (If yes, check and verify how such websites are blocked.)

21

- Are children allowed in the cybercafe for playing computer games?
- If yes, is the access to the Internet blocked? (If yes, check and verify how access to the Internet has been blocked.)

22 Do you get the user access logs from each computer system?

- Are these user access logs preserved? If yes, for how many days/months/years these logs are preserved?
- If yes, check and verify for each computer system if following details are captured in the logs:
  (a) IP Address of each computer system;
  (b) Websites visited by each user.

23

- Is the cybercafe registered with Cyber Cafe Association of India (CCAOI)?
- Do you get any training, related with cybercafe management, from CCAOI after registration? (If yes, is the training includes any modules on cybersecurity?)
- Do you get required support from CCAOI?
- Do they (CCAOI Officials) conduct any visits and/or audits to the cybercafe? (If yes, how frequently monthly/bi-annually/annually.)

24

- Do you get required support from cyber police?
- Do they (cyber police) conduct any visits and/or audits to the cybercafe? (If yes, how frequently monthly/bi-annually/annually.)

25	Have you received any guideline about cybersecurity from CCAOI/cyber police/Internet Service Provider?

This checklist can also be used, with few alterations, for the computer systems available with the Internet in public places such as libraries, hotels, holiday resorts, etc. to assess the due diligence toward established cybersecurity measures.

After the assessment, based on the results, cybercafe owners/operators may seek an advice to implement the computer software that will help them to monitor security aspects for entire cybercafe as well as monitor the time for each cybercafe user for invoicing (i.e., billing). The computer software(s) mentioned below are the known utilities in India, which are designed and developed for day-to-day management of cybercafe operations.

1. **Webcafe ERP:** www.rhombustechnologies.com
2. **CLINCK Cyber Café Manager:** www.clinck.in

In summary, cybercafe owners/operators should implement security measures to protect cybercafe users, and Netizens as an individual should also take utmost care while visiting and/or operating from cybercafe to avoid being a victim of cybercrime. Few tips toward safety and security for netizens are explained in Section 2.5 in Chapter 2.

Further Reading

Articles and Research Papers

1. Whitepaper on *Cyber Crime and Criminality in Nigeria – What Roles are Internet Access Points in Playing?* by Longe, O.B and Chiemeke, S.C.
2. Read article *Beware of Cyber Threats in A Cyber Cafe* at: http://www.troublefixers.com/security-tips-for-cyber-cafe-usage/ (10 January 2011).
3. Whitepaper on *Cyber Café Surveillance* by Vats, Y. and Rathore, D. can be accessed at: http://www.scribd.com/doc/34488348/Whitepaper-on-Cyber-Cafe-Surveillance (10 January 2011).