Merchants' Chamber of Commerce & Industry

Workshop on "Protection Against Cyber Crime & Hacking"

on 11th August 2018 at 11.00 AM at MCCI Conference Hall

Brief Proceedings

The Chamber organized a **Workshop on "Protection Against Cyber Crime & Hacking"** on Saturday, 11th August, 2018 at MCCI. The Workshop was addressed by **Shri Sandeep Sengupta,** Cyber Audit Expert & CEO, Indian School of Anti Hacking (ISOAH) Data Securities Pvt. Ltd.

The Workshop covered the following areas :

- Why organizations/ individuals get hacked
    - Common attacks, future attacks and threats through wifi at office/ home
    - Other threats involving debit/ credit cards & net banking
    - Hacking of devices, email/ Facebook/ Whatsapp & other ids
- How to prepare for a hack proof organisation
    - Protection & Privacy of data and Personal Safety
    - System Security Audit

- Shri Sandeep Sengupta mentioned that Cyber Security had been a subset of Information Security, in which all the verticals in a business organization like Admin, HR, Accounts, Marketing, Legals – have huge roles to play. He said that the ways of doing business would change drastically with technology and enhanced bandwidth. He stressed on PPT: People, Process & Technology.
- He suggested that it would be important to generate awareness regarding the possible dangers of cyber crime and hacking. There should be annual awareness sessions in organizations. In schools and educational institutes, priority importance should be accorded to Teachers' Training programmes to guide the students, he noted.
- He advised all to be careful about contact less cards and suggested to wrap it in aluminium foils/ boxes, to protect the same from being hacked.
- He urged not to share the mail password/ wifi password/ PIN to anybody and advised all to change the same on a regular basis, once in 30 days.
- In case of mail spoofing, there would be a reply marked to gmail or yahoo or any other public id. He felt that filtering emails would create an additional layer of security.
- He warned all of call spoofing and said that if the accounts department is asked any confidential information, then the person concerned should call back the caller.
- To stop ransomeware, LAN should be segregated, as it is important to have physically separate VLANs.
- For HR, he observed that for evaluation of recruits, Risk = Likelihood x Impact. He said that while doing the background checking, obtaining a Police Clearance Certificate by the

incumbent should be made compulsory, as this would drive away those having criminal records. For recruitment of security guards, the candidates could be asked to give a family photo as background check. For Non–Disclosure Agreements, the timeline should kept even after termination of job.

- There should be a proper exit policy for employees and the Asset Return Form should include Laptop and other devices, Biometric and should involve changing all the passwords, blocking access to information from different Departments like IT/ Finance/ Admin/ HR/ Marketing and others.
- For IT & software companies, he advised that the source code should be loaded on the virtual machine and not on individual person al machines. He stressed on DRM (Digital Right Management) software and also emphasized on regular backups.
- He pointed out that physical security is important and there should be material management register with page numbers, so that pages are not torn from the middle.
- There should be a Visitor Register at the Gate and also at the Server Room, he opined.
- He felt the unsuccessful attempts at the biometric machine should be reviewed periodically. In a BPO/ Finance, no CCTV should focus on the screen, he added.
- He advised ISO 270001 for all for Risk Identification.
- He mentioned that there should be different sets of people for risk identification and risk mitigating. People entrusted with identifying risks should not be burdened with mitigating the same, as that would induce them to start skipping risks.
- He stressed on the People & Process part in an organization and felt that every document should have a document classification.
- As a part of change management, he emphasized that all the access rights should be reviewed at least quarterly and all passwords changed.
- He referred to a Tool called **NESSUS**, free for 16 IP addresses and advised all to download this and run a month in the network. He felt that Nessus is good for infrastructural, networking and patching issues, but not for coding problems.
- He spoke about another open source software, **KALI LINUX** for software audit, which point out mistakes in the system. There are more than 500 tools, but one tool VEGA would be good enough for pin pointing the misses in the system.

The Opening Remarks were delivered by **Shri Sanjib Sanghi**, Co Chairman, Standing Committee on IT & Communication of the Chamber.

The Workshop was attended by representatives of the member–firms of the Chamber as also a few select non–members.

****

Munmun Banerjee
Assistant Director General