PAROMITA BANERJEE SEN
and
SOUMEN SEN

Cyber security issues in Indian economy

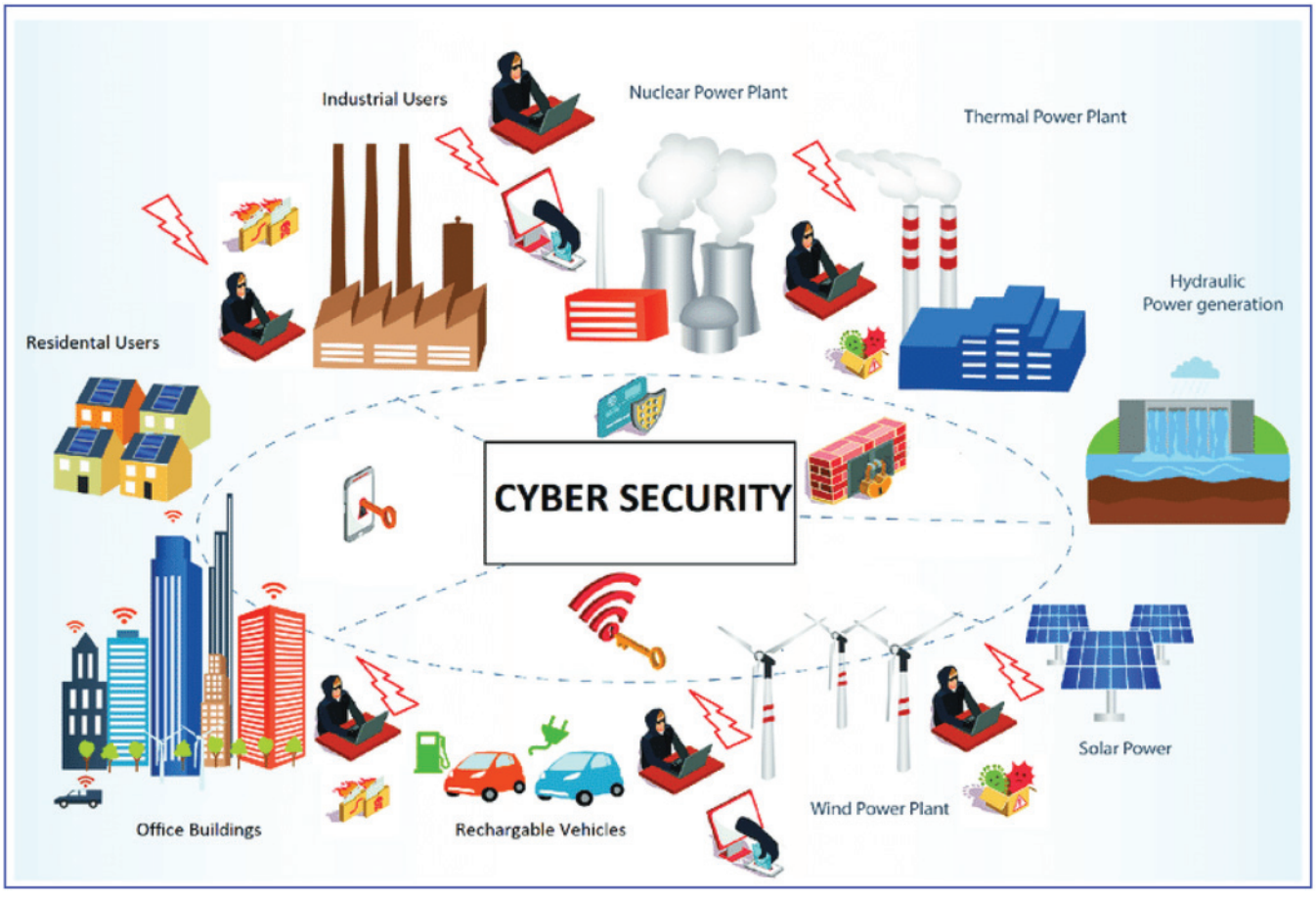

Fig.1: Block diagram of cyber secure network

The more we are marching towards a digital future, more prone are we to cyber security issues. As the Android phones are upgraded to 5 G, more susceptibility to cyber security issues are there. The organisation security is at stake. There are various types of attackers like – White Hat, Gray Hat and Slack Hat and organised hacking mechanism is on the way. The paper highlights on the types of malwares and how we are trapped in the network by virtue of improper knowledge. The hardware and software vulnerabilities will enable us to be prone to cyber attacks.The paper will highlight the loopholes of the existing system and suggest measures to remove the obstacles for a Economy free of cyber threats.

Keywords: White Hat, Malware, Vulnerability.

Ms. Paromita Banerjee Sen, Damodar Valley Corporation, Raghunathpur Thermal Power Plant, Purulia and Mr. Soumen Sen, Department of Electronics and Communication Engineering, Asansol Engineering College, Kanyapur, Vivekananda Sarani, Asansol 713305. E-mail: paromita.banerjee@dvc.gov.in

Introduction

The need of cyber security is that we need to identify the attackers, intruders, value of data and its security, We can protect our devices by turning firewall on and updating firewall, installation and update of antivirus, manage security settings of browsers and password protect sensitive data.

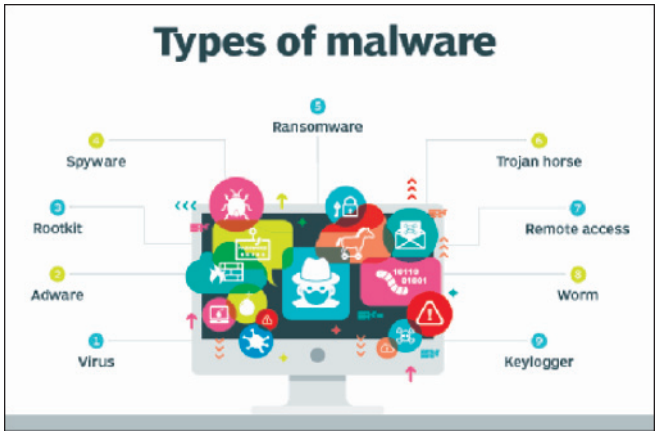

Fig.2: Types of malware

Theoretical Details

Types of attackers:

1. White Hat – They use their skill to protect against attacks.
2. Black Hat – They are malicious attackers with evil intentions.
3. Gray Hat – They are a combination of both black and white hackers.

A. Spyware – This type of malware spys/tracks all online activity along with legitimate software/Trojan horses.

B. Adware – adware comes with advertisement. Adware comes together with spyware.

C. Backdoor – It gives remote access to intruders. It works in background and difficult to detect.

D. Ransomeware – System encryption is captive until ransom is paid.

E. Scareware – In this malware, scare tactics run the programme.

F. Rootkit – Software vulnerability access remotely.

G Trojan Horse – It sneaks malicious software image, files, audio and games.

H. Worms – These malwares can run by themselves. The most devastating was Red worm of 2001.

The vulnerabilities are of 2 types:

1. Hardware vulnerability
2. Software vulnerability

A programme written to take advantage of a known vulnerability is exploit. A cybercriminal can use an exploit against a vulnerability to attack. Security vulnerability is a software or hardware defect.

Data Back Up

The increasing trend of cyber security demands data back up.The data can be backed up in home network. Secondly it can be backed up in network attached storage devices like hard disk CD/DVD. Thirdly Cloud Storage systems ensure data is safe in times of theft of device or device failure.

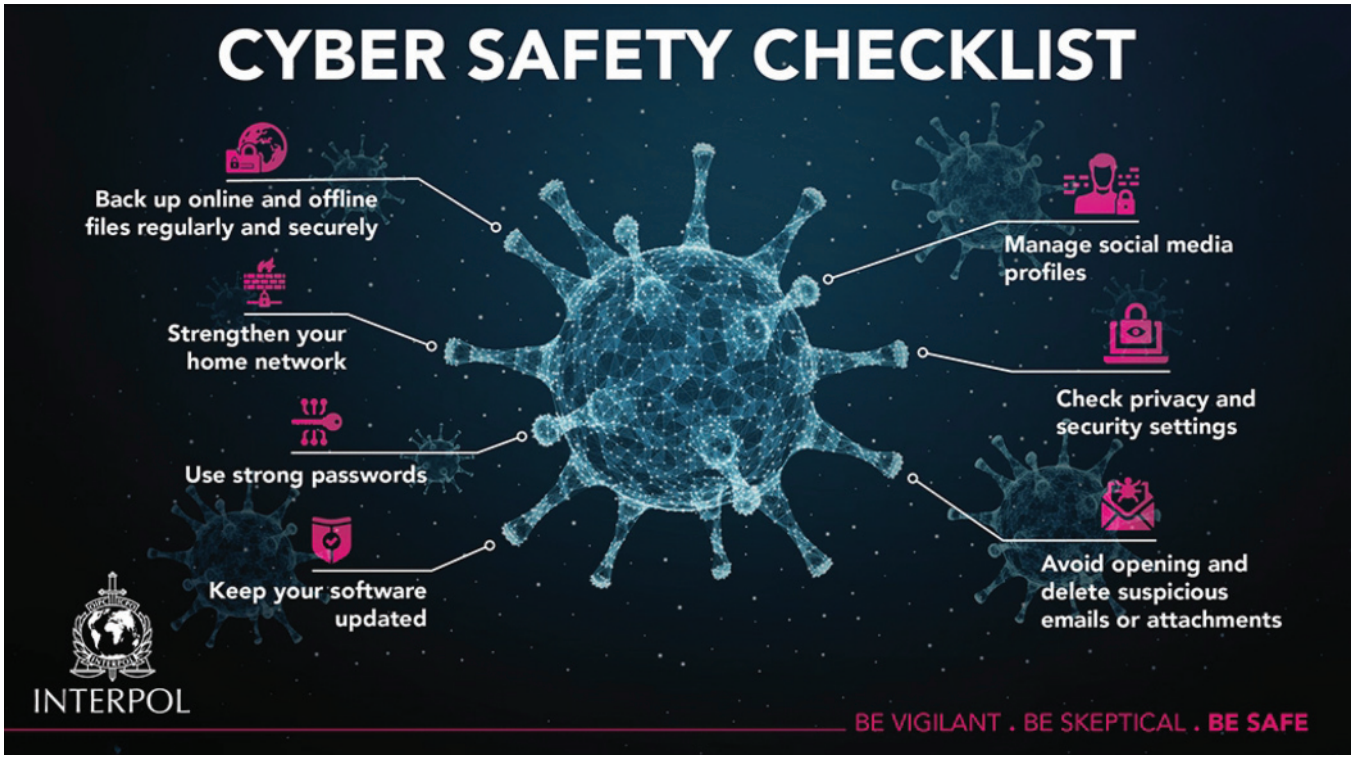

Fig.3: Cyber Security in environment

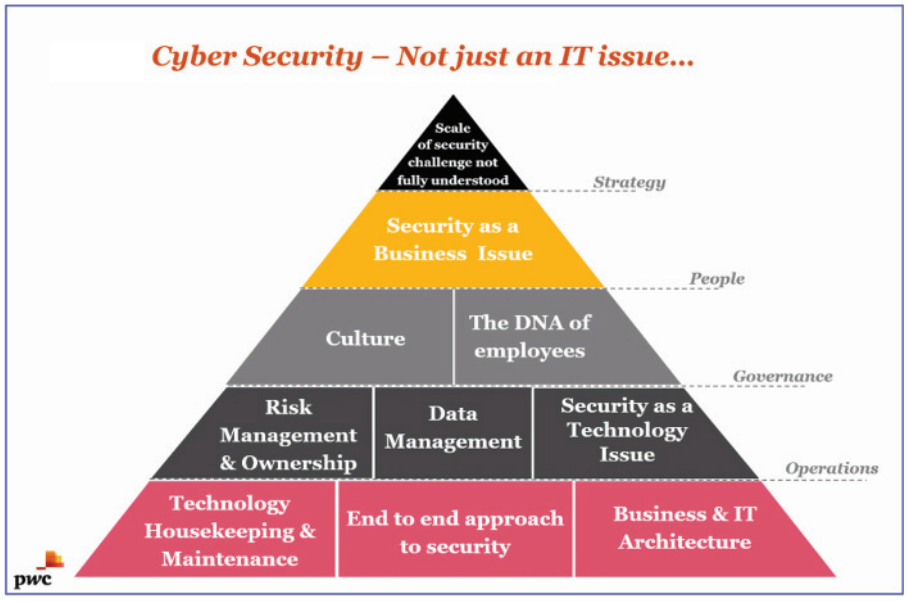

Fig.4: Organisation structure

Data deletion

When we delete items in desktop/laptop, the data is not properly erased. Anyone with right forensic tools will still recover due to magnetic traces on hard drive.

Data must be overwritten with 1/0 using specific tools . The hard disk has to be destroyed completely to delete the data permanently.

Organisation Protection

1. Routers – while they are used to interconnect various network segments together, they provide traffic filtering capabilities . It is the pathway which network can connect with network segments.
2. Firewalls – They look deep and identify malicious behaviour to be blocked. Firewalls can have sophisticated security policies applicable to traffic.
3. IPS – Intrusion Prevention Systems use a set of traffic signatures that block malicious attacks.
4. VPN – Remote employees use a secure encrypted level from their mobile. It can connect branch offices with central office.
5. Antimalware/Antivirus – They block malicious code from being executed.
6. Other security measures – Web and security applications, decryption devices, client access control servers and security management systems.

Organisation Policies

The policies which an organisation makes help it to become cyber secure. It includes – Risk assessment, security policies, human resource training, updation of security packages and educate its employees agrainst potential cyber threats.There should be a team of cyber security experts with incident response and threat intelligence to manage cyber security issues prudently.

Conclusion

In any organisation which is big or small, a stitch in time saves nine. Cyber security measures with risk factors, system vulnerability are to be addressed in time to minimise sacrifice of data. It is likely in the near future the most demanding profession of any ecomomy because we are moving towards a digital world.

References

[1] Collier, S. E. (2010): Ten steps to a smarter grid. Industry Applications.

[2] Magazine, IEEE, 16(2), 62-68H. Simpson, Dumb Robots, 3rd ed., Springfield: UOS Press, 2004, pp.6-9. IEEE Std. 999-1992, "IEEE Recommended Practice for Master/ Remote Supervisory Control and Data Acquisition (SCADA) Systems," *Institute of Electrical and Electronics Engineers*, 1992.

[3] Hongchun Yao; Qiwei Peng; Weiguo He; Xinlong Zhang, "Integrated Cmunication Technology for Supervisory Control and Data Acquisition System of PV Power Station", Intelligent System Design and Engineering Application (ISDEA), 2012 Second International Conference on, pp. 1277-1280, 2012.

[4] Khairy Sayed, and Hossam A. Gabbar, "Smart Energy Grid Engineering", pp.481-514

[5] Hirofumi Terada; Tsukasa Onishi; Tatsuhiro Tsuchiya, "A monitoring point selection approach for power distribution systems", System of Systems Engineering (SoSE), 2013 8th International Conference on, pp.190 - 195, 2013.

[6] Google pictures on cybersecurity.

Printed by Pradip Kumar Chanda at The Indian Press Pvt. Ltd. 93A Lenin Sarani, Kolkata 700 013 and published by him for Books & Journals Pvt. Ltd. from 62 Lenin Sarani, Kolkata 700 013