Workshop Report

1) **Workshop Title** : Workshop on Emerging IT & Cyber Security challenges for IT Heads of Cooperatives.

2) **Mode of programme**- Off-Line

3) **Date / Duration**: **19th – 20th October, 2023** (2 days)

4) **Number of participants** – 14

5) **States Covered in Programme** – Maharashtra

6) **Need and Importance of Program** : The major sectors of cooperatives viz Banking, Sugar & dairy have established IT set up & trying to keep space with technological advancements & have invested in deployment of latest hardware & software required infrastructure. However, the required qualified & experienced manpower is still not been seriously looked into by cooperatives. Due to non availability of technical manpower the IT & cyber security threats are on the higher side in cooperatives as compare to other sectors. In absence of IT & Cyber Security requirements many cooperative banks have faced cyber attacks on their IT set up which has also resulted in reputed risk to these cooperative banks. In this context, the sensitization on IT & Cyber security insights to available technical manpower of the cooperatives is of paramount important in order to secure the IT environment & minimize IT risk the contents of the workshop are therefore quietly useful in taking appropriate security policy & cyber security policy & security solutions.

7) **OBJECTIVES OF WORKSHOP**
   - To acquaint with emerging cyber security challenges To discuss cyber security preparedness
   - To assess the level of security & solutions thereof
   - To define requirements of IT & Cyber security policy & cyber insurance.

8) **Session Details (Inclusive of No. of sessions with 7-8 lines brief about each):**

1) Drafting of IT security & Cyber Security Policy: The session was delivered by Dr. Y.S. Patil, Programme Director.

Dr. Y S Patil commenced the session by explaining the concepts of Policy Statements and procedures. He mentioned that IT Policies and procedures build the foundation for technology use practices. IT policy defines how an organization aims to implement, operate, and manage technology in a way that enables the organization to meet legal and regulatory requirements. The procedure outlines a plan of action for implementing a policy.

- Dr. Patil the explained the various IT Policies that must be in the place for cooperative bank and cooperative sugar factories. The important policy inclusions are the information security, IT Governance, Network and computer use, Security awareness and training to the employees, Incident response, Remote Access Policy, Email Policy, BYOD policy, Data Backup Policy etc. These IT policies and procedures guide the organization on various aspects of implementing IT the right way.
- Further, Dr. Patil explained the advantages of documenting the IT Policies and Procedures. The IT policies should set clear expectations of what needs to be performed in their specific job roles. Good policies need to be established for regular training, responsibilities, access to critical information, performance and more. The IT security policy & cyber security policy has to be distinct. These policies have to approved by the management and has to be in simple language for undertaking of users. The policy has to implemented across the organization via branches, regional offices etc. Dr. Patil explained that the policies heads to be review on periodic basis and needs to updated from time to time for its relevance and needs to audited.

2) **Elements & Types of Cyber Security- Application Security, Information Security, Network Security, Operational Security, Mobile Security, Cloud Security**: The session was delivered by Shri Nachiket Pohekar, Manager-IT, COSMOS Cooperative Bank LTd., Pune

- Shri Pohekar explained the IT Security which is a set of Cyber Security strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. It maintains the Confidentiality, Integrity and availability of all information assets of the organization.
- While addressing the participants, the speaker discussed the Best practices for IT operational Security like Update all desktop, laptop and end points with latest anti-virus and anti-malware, to educate the user about to how to check the updated anti-virus on all computers, use active directory solution for end user authentication and authorization, to enable the 2FA authorization for all user login to the bank system, to update the critical and security patches of OS on real time basis etc.

- He emphasized the need of infrastructure required for IT security like NG- Firewall, Host based intrusion prevention system, Anti-bot /Anti malware solutions, Honey pot / deception technology, DNS /AD/ PRXOY / MAIL Server security etc.
- He highlighted the various steps that the top management of the organization should take in order to implement successful cyber security operations.
- Shri Pohekar explained the Cloud Security framework for Indian Banking Sector. He described that there are several Cloud security standards and guidelines which describe the various aspects of security in the Cloud environment. While reviewing those security standards and guidelines, to the best of knowledge there are no Cloud security best practices, and guidelines that meet the complete needs of Indian Banking and Financial Institutions. Hence a set of guidelines and best practices are developed describing IDRBT Cloud Security Framework as a practical, simple and easy to use guidebook that will help banks to understand and explore security concerns in the Cloud environment.
- Shri Pohekar demonstrated the freely available security tools and techniques which can be used for assessing the security threats.

3) **Cyber Security Tools & Techniques and Cyber Security – Risk Management & Cyber Insurance**: The session was delivered by Shri Nachiket Pohekar, Manager-IT, COSMOS Cooperative Bank LTd., Pune

4)

4) **Information Security & Cyber Security Challenges**: The session was delivered by Dr. Sanjay Shinde, IPS, Joint Commissioner of Police, PCMC, Pune

- Dr. Sanjay Shinde elaborated on the topic of information and cyber security, He highlighted that the goal of cyber security is to protects against unauthorized access and the goal of information security is to protects the confidentiality, integrity, and availability of all types of information. He further added that Cybersecurity deals with the danger in cyberspace. Information security deals with the protection of data from any form of threat.
- Dr. Shinde also highlighted the vulnerabilities that can perform unauthorized actions within the computer system. He explained the vulnerabilities classification in hardware, software, network, personnel, physical sites and organizational.
- Further, Dr. Shinde highlighted on the topics of deliberate software attacks, Malwares, Distributed Denial of Services (DDoS), Phishing (Email) & Vishing (Phone calls).

- He explained the common types of crimes that occur related to cyber security viz, compromises to Intellectual Property, Espionage/Trespass, Information Extorsion, Sabotage or Vandalism, deliberate acts of Data Theft etc.
- Dr. Shinde also highlighted the protective measures that can be taken to mitigate risk. The security frameworks play a significant role in mitigating cyber threats by making the path to implementing security controls, policies and procedures easier. He also shared the cybersecurity tips and best practices that can help from security threats band vulnerabilities.

Commencement of Presentations:

14 Participants were divided into 4 groups. Each group had a topic on which they were suggested to give a presentation. The 4 groups were formed as per the details given below:

Group 1

Topic : Elements & Types of Cyber Security- Application Security, Information Security, Network Security, Operational Security, Mobile Security, Cloud Security

1) Shri Vijay Prabhakar Ambilwade, EDP Manager
2) Mrs. Jaishri Pankaj Bhoir, Officer JM
3) Mrs. Deepali Sanket Padwal, Jr. Officer
4) Shri Krishna Mohan Vadak, IT Support Executive

Group 2

Topic : Cyber Security Tools & Techniques

1) Shri Patil Sanjay Baburao, Manager IT
2) Shri Shahane Kiran Laxman , EDP Manager
3) Shri Harshal Ramdas Mhatre, IT Officer

Group 3

Topic: Cyber Security – Risk Management & Cyber Insurance

1) Shri Kharatmal Sandip Narsingh, IT Officer
2) Shri Vikram Jijaba Khabale, Software Engineer
3) Shri Bhaskar Mohan Desai, Asst. Manager

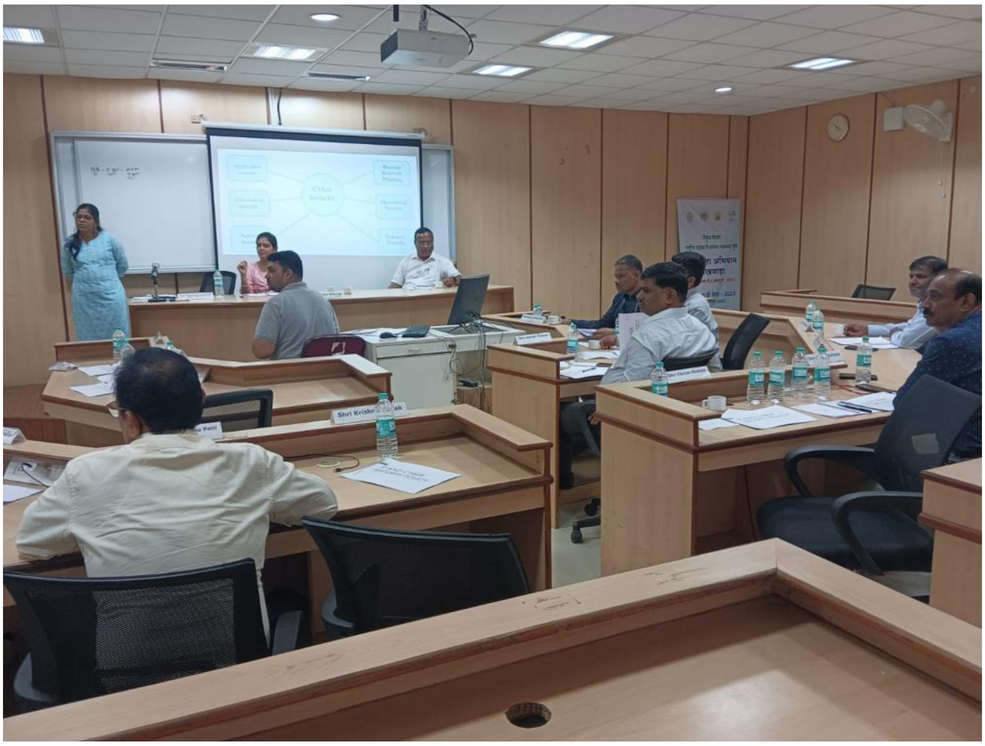
Group 4

Topic: Drafting of IT security & Cyber Security Policy

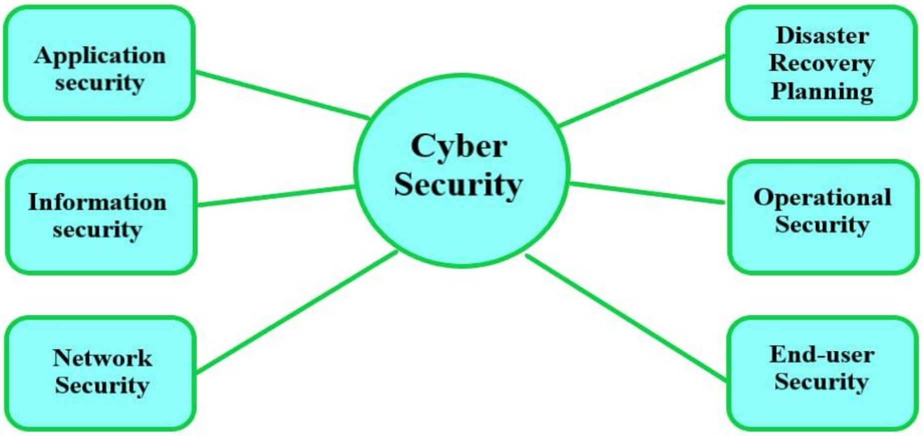
1) Shri Sachin Ramchandra Jamdar, Manager MM-II (IT)
2) Shri Ashish Shaligram Chavan, Assistant Manger IT
3) Shri Nilesh Yashwant Nabar, Asst. Manager
4) Shri Nivrutti Karbhari Abhale, Clerk

Group 1

Topic: Elements and types of Cyber Security



As a part of the workshop, a group of following officials discussed and presented the group opinion on the theme '**Elements and types of Cyber Security'**. The session was chaired by Shri Nachiket Pohekar, Manager-IT, COSMOS Bank.



The group expressed on following aspects-

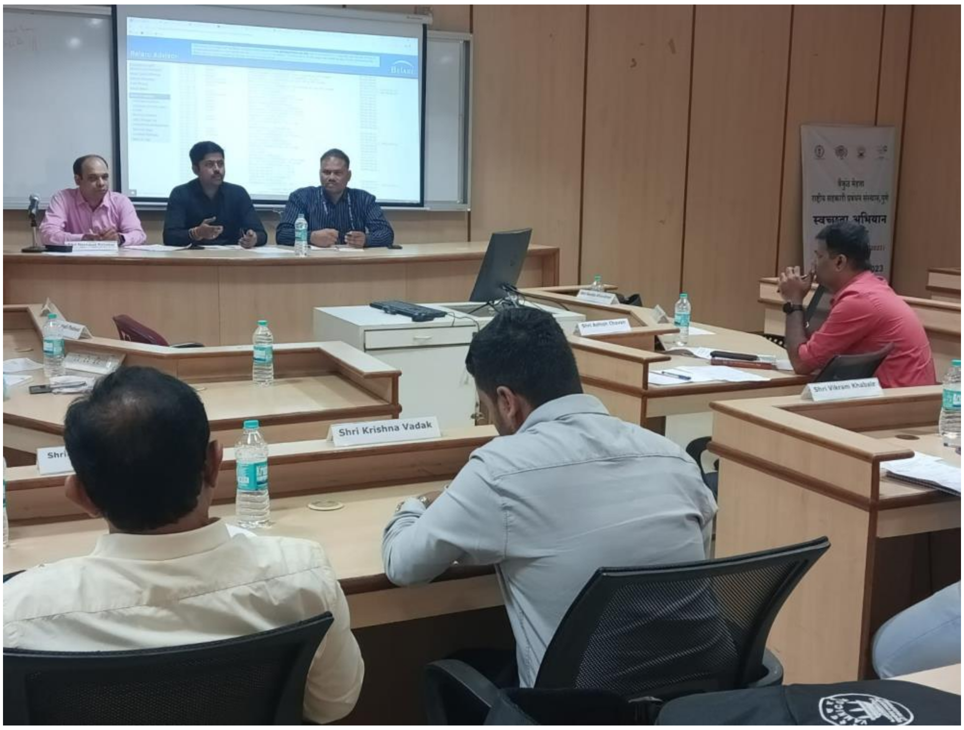
- The group explained the different elements of Cyber Security like Application security, Information security, Disaster Recovery Planning, Network Security, End-user Security and Operational Security.
- The group felt that, every firm needs to focus on application security as it plays an essential role in organization. An organization protects its customers, assets, and interests by protecting applications. But the main challenge is the identification of vulnerabilities within the parent system. If these vulnerabilities are exposed to attackers, they can be exploited to gain valuable insight into the functioning of the application.
- The group highlighted the challenges in developing a comprehensive cybersecurity strategy due to the rapidly evolving nature of cyber threats and the complexity of the cyber infrastructure.

- One single security breach can lead to exposing the personal information of millions of people. These breaches have a strong financial impact on the companies and also loss of the trust of customers. Hence, cyber security is very essential to protect businesses and individuals from spammers and cyber criminals.

Group 2

Topic: Presentation on Cyber Security Tools and Techniques

Session Chair: Dr. Y S Patil, Associate Professor, VAMNICOM



- The presentation by explaining various Cyber Security Tools used in their organization. The following security tools which are freely available were discussed in the session.
  1. **SIEM** - SIEM software, tools and services detect and block security threats with real-time analysis. It allow organizations to efficiently collect and analyze log data from all of their digital assets in one place
  2. **DLP Tools** - DLP tools constantly monitor and analyze data to identify potential violations of security policies and, if appropriate, stop them from continuing.
  3. **D Shell** - It is an extensible network analysis framework. It enables rapid development of plugins to support the dissection of network packet captures.
  4. **Wireshar**k - Wireshark is a software tool used to monitor the network traffic through a network interface. It is the most widely used network monitoring tool today.
  5. **Burp Suite** - Burp Suite is a set of tools used for penetration testing of web applications. Burp Suite is a platform and graphical tool that work together to do security testing on online applications. It supports the whole testing process, from the initial mapping and analysis of an application's attack surface through the discovery and exploitation of security vulnerabilities.
  6. **TCP Dump** - The tcpdump utility is used to capture and analyze network traffic. Sysadmins can use it to view real-time traffic or save the output to a file and analyze it later.
  7. **eScan Cert**- in Bot removal - The app will scan your device for malware and remove any infections that are found

- In view of this, the groups complained the cyber-criminals who continue to expand their techniques and level of sophistication to breach businesses security, it has made it essential for organizations to invest in these training tools and services. Failing to do this, they can leave the organization in a position where hackers would be easily targeted their security system. So, the expense of the investment on these training tools might put a reward for the business organization with long-term security and protection.
- The team opiniated that, many training tools available that can educate company's staff about the best cybersecurity practices. Every organization can organize these training tools to educate their employee who can understand their role in cybersecurity.

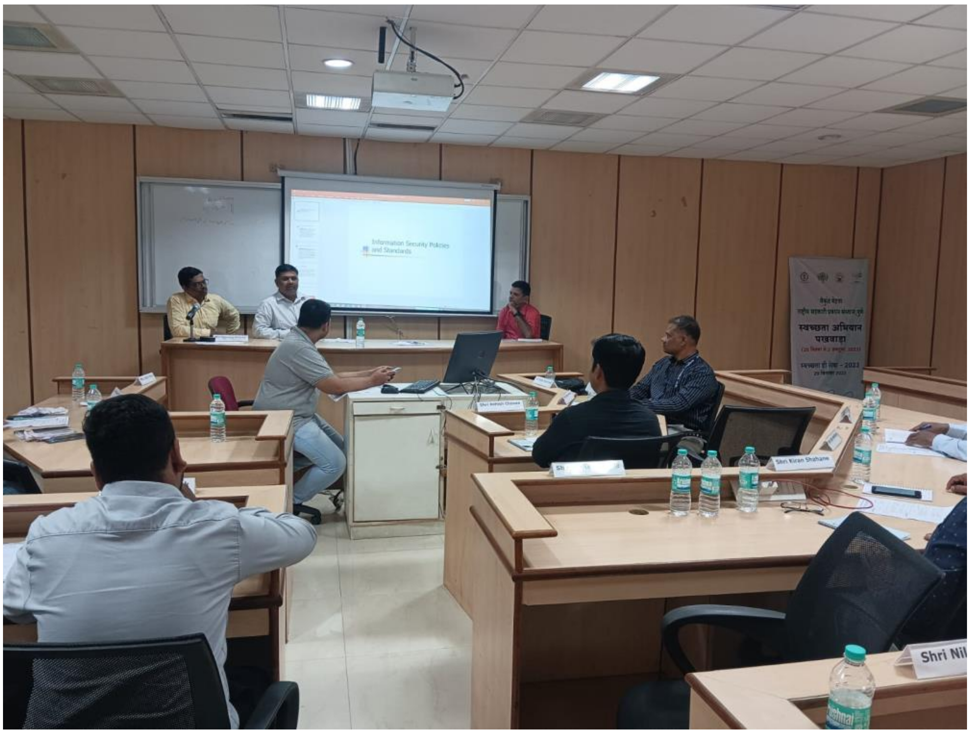
Group 3: Presentation on Cyber Security - Risk Management add Cyber Insurance
Session Chair : Shri Ajay Nikunb, IT Consultant

- Shri Ajay Nikunb explained the techniques of performing the Cybersecurity Risk Assessment. He explained two methods for assessing risks, viz confidentiality, integrity and availability (CIA) method and Process based risk assessment. The group Shri Nikunb discussed on the asset value for assessing the worth of the organization's information system assets can be calculated based on its CIA security. The values can be used to identify the threats that can occur in the system and its impact.
- The Process based risk assessment allows the user to list all the processes of the system. For each process, data flow diagrams are generated and for each of these diagrams the risk assessment is done.
- Shri Nikunb explained the various CIA triad used in the organization. Protecting information from unauthorized access and disclosure, protecting information from unauthorized modification and preventing disruption on how information is accessed and some of the CIA triad to protect the stakeholders from threats and vulnerabilities.
- During the session, Shri Nikunb answered queries raised by the participants. The techniques for selecting the secured cloud was explained during the session.
- The session concluded by highlighting the importance of cybersecurity risk as it can help identify risks to organization's information, networks and systems. By identifying these risks, one can take steps to mitigate or reduce the risk. A risk assessment can also help your organization develop a plan to respond to and recover from a cyber-attack.

Group 4: Presentation on Drafting of IT security & Cyber Security Policies

Session Chair: Dr. Y S Patil, Associate Professor, VAMNICOM

The group presented on the theme '**Drafting of IT security & Cyber Security Policies**'



The group expressed on following aspects-

- The group shared concerns with respect to the Security policies used in the organization. The team gave a presentation on Information security Policies and the challenges faced in defining the security policies and standards, correct violations to conform with policy, the policy compliance fir the organization.
- The group explained the various elements of policies and its lifecycle.
- The group members also highlighted the ten-step Approach for setting the policies and standards in the organization, which includes Collecting the background information, performing the risk assessment, developing the Information Security Plan, developing Information Security policies. implementing policies and standards, awareness and training, monitor for compliance etc,
- A cyber security policy has far-reaching impact across the organization and can touch multiple departments. For example, IT staff may be responsible for implementing the policy, while the legal or HR teams may have the responsibility for enforcing it to ensure that the policy implementation delivers the expected objectives.

9) **Suggestions and feedback : in 7-8 lines approx**

In the concluding of the workshop, participants from State Cooperative Bank, District Cooperative Banks, Urban Cooperative Banks and Cooperative Sugar factories expressed their views on contents and delivery of the sessions. The participants suggested to increase duration of the programme and expressed their satisfaction for overall conduct of the workshop and arrangements lodging, boarding and classrooms.

Dr. Hema Yadav, Director, VAMNICOM addressed the participants highly by the initiatives of Ministry of Cooperation in digitalization of conceptual and other technology initiatives. Dr. Y.S. Patil, workshop Director presented vote of thanks.

(Y.S. Patil)
Programme Director