



# Institute for Development and Research in Banking Technology

(Established by Reserve Bank of India)

Castle Hills, Road No. 1, Masab Tank, Hyderabad-57, India.

---

e-Programme on

## **PROACTIVE CYBER DEFENCE STRATEGIES**

**NOVEMBER 29 – December 02, 2022**

---

### Introduction

The cyberattacks or incidents are increasing exponentially in number as well as in strength, variety and impact. Due to that, the organizations' reputation and business continuity are at stake. Earlier, due to several reasons (such as overconfidence in their cyber resilience, ill-advised, unawareness etc.), many organizations followed reactive defence strategy and ignored the long-term losses and recovery process from cyber-attacks.

For instance, in reactive defence strategy, while dealing with the NotPetya malware, all the hazardous applications identified as the source of the outbreak will be isolated. Short-term stop-gap solutions could be installing/reconfigure the firewall, DLP solutions, anti-malware applications. Therefore, the reactive approach is heavily attack-dependent, thus failed to provide a reliable solution.

It is high time to move the needle on proactive cyber defence from the reactive strategy. In proactive cyber defence, an organization needs to see from where threats are coming, how they can move within the network, how much it can exploit the systems, where the vulnerabilities are present in the defences. Find and mitigate/close those before the attackers can take any advantage.

### Objective

The objective of this e-Programme is to enlighten the participant regarding proactive cyber defence strategy, its benefits over-reactive strategy, different proactive cyber defence exercises such as vulnerability assessment, breach & attack simulation (BAS), penetration testing, red team vs. blue team, cyber drill and cybersecurity exercise. It will help the banks to strengthen their cyber defence provisions.

### Contents

- Cyber Exercise
- VA vs. PT vs. BAS
- Cyber drill, Red Team vs. Blue Team exercise, Bug bounty
- Tools and resources for cyber defense, Honeypot
- Case study

### Mode of Teaching

Online teaching plus learning inputs through reading material, videos, webinars, assignments, quizzes, online interactions and clarifications. Each e-Programme will have four live webinars and course material will be made available in advance for study.

## Who Can Participate?

Bank officials working in IT Department, cyber Security Operations Centre, Network operations Centre and related activities.

## End Use:

This e-Programme will help the participant strengthen their knowledge and awareness of cyber security and help the banks improve their cyber defence provisions.

## Programme Coordinator:

**Dr. Dipanjan Roy**, Assistant Professor, IDRBT; e-mail: [droy@idrbt.ac.in](mailto:droy@idrbt.ac.in)

## Fees:

### **For Indian Participants**

- RRBs & Coop Banks: Rs. 11,800/- (Rs. 10,000/- + 18% GST)
- All Other Banks & Financial Institutions: Rs. 14,750/- (Rs. 12,500/- + 18% GST)

### **For International participants**

- US \$ 220 (per participant, All inclusive)

## Bank Account Details for Remittance of Fees

The fees for this e-programme can be remitted to the following accounts:

### **For Indian Participants**

Account Name : IDRBT  
Bank & Branch : Axis Bank Limited, Humayun Nagar, Mehdiapatnam, Hyderabad  
Account No. : 426010100018823  
MICR Code : 500211012  
IFSC Code : UTIB0000426

### **For International participants**

Receiver's Correspondent Bank : JP Morgan Chase, New York, USA  
Swift Code : CHASUS33XXX  
Fed Wire Routing Number : ABA 021000021  
Beneficiary Bank & Branch : Axis Bank Ltd., Mumbai, India  
Account Number : 0011407376  
Beneficiary Bank Swift Code : AXISINBB

### **Ultimate Beneficiary**

Account Name : IDRBT  
Customer ID : 030021632  
Account No. : 426010100018823  
Bank & Branch : Axis Bank Ltd., Jubilee Hills, Hyderabad, India. (AXISINBB030)

## Nominations

Banks may nominate any number of participants to these e-Programmes, which may be accepted on a first-cum-first-served basis. While nominating, please provide the details of the participants (Name, Designation, Bank, Mobile No/Phone No, email address, fees billing address, GST No. of the Bank).

Apart from nominations by banks, staff members of banks can self-nominate themselves for these e-Programmes by providing their employee credentials and paying the programme fee latest by **November 28, 2022**.

## How to Register

The nominations for these e-Programmes, and queries if any, may please be sent to [eprogram@idrbt.ac.in](mailto:eprogram@idrbt.ac.in). Please visit <https://www.idrbt.ac.in/eprogrammes> for more details about these programmes.

\*\*\*\*\*

### e-Programmes in November 2022

S. No.	Name of the e-Programme	Date	e-Programme Coordinator	Last Date for Nomination
1	Emerging Banking Technologies	22 – 25	Dr. Rajarshi Pal	<b>Nov 21, 2022</b>
2	Inside Threats - Detection and Prevention Techniques	Nov 29 – Dec 02	Dr. B. M. Mehtre	<b>Nov 28, 2022</b>
3	Governance, Risks and Compliance	Nov 29 – Dec 02	Dr. Abhishek Thakur	<b>Nov 28, 2022</b>
4	Future of Innovative Smart Banking	Nov 29 – Dec 02	Dr. Susmita Mandal	<b>Nov 28, 2022</b>
5	Proactive Cyber Defence Strategies	Nov 29 – Dec 02	Dr. Dipanjan Roy	<b>Nov 28, 2022</b>

### e-Programmes in December 2022

S. No.	Name of the e-Programme	Date	e-Programme Coordinator	Last Date for Nomination
1	Technologies for Financial Inclusion	05 – 08	Dr. M. V. N. K. Prasad	<b>Dec 02, 2022</b>
2	RBI Guidelines on Cyber Security	06 – 09	Dr. Dipanjan Roy	<b>Dec 05, 2022</b>
3	Re-envisioning Digital Banking Systems	13 – 16	Dr. Susmita Mandal	<b>Dec 12, 2022</b>
4	Big Data and Cloud	19 – 22	Dr. P. Syam Kumar	<b>Dec 16, 2022</b>
5	Continuous Security Validation	20 – 23	Dr. V. Radha	<b>Dec 19, 2022</b>
6	Applications of Dark Web	27 – 30	Dr. B. M. Mehtre	<b>Dec 26, 2022</b>
7	Cyber Security for Remote Working Scenario	27 – 30	Dr. Rajarshi Pal	<b>Dec 26, 2022</b>