momenta
leadersdrivingperformance

IBF-STS

Pending Accreditation

IN-PERSON WORKSHOP

Data Privacy & Cybersecurity Protection – Practical Tips Beyond Firewalls

Target Audience:
Private Bankers, Wealth Managers, Financial Advisors, Retail Bankers

Duration: 4 CPD Hours

Core FAA/SFA Hours: 4

Fee: SGD 650 per participant

EARLY BIRD DISCOUNT

Enjoy **10% discount** when you register **one (1) month before** the course commencement date.

Learning Objectives

- To strengthen professional awareness and judgement in managing data privacy and cybersecurity risks, prevent breaches through real-world case analysis, and build a culture of trust and digital accountability across client interactions.

What you'll learn

1. Cyber Investigator HAT – Starting Exercise

- Recognize common cyber threats such as phishing, malware, and insider leaks through real-world mini scenarios.
- Assess each case by threat type, potential impact, and preventability to sharpen risk awareness.
- Identify which threats pose the greatest danger and discuss preventive actions as a team.

2. Cyber Investigator HAT – Spot the Weak Links

- Analyze a real financial-services breach to uncover human and system-level weaknesses.
- Identify key red flags, control failures, and missed preventive measures.
- Discuss practical steps bankers can take to detect and stop similar threats early.

3. Client-Facing Banker HAT – Beyond Firewalls

- Translate complex cybersecurity principles into simple, client-friendly language.
- Practice explaining safe digital habits and preventive measures during client interactions.
- Build confidence in promoting data security while maintaining trust and professionalism.

4. Client-Facing Banker HAT – Human Layer of Security

- Examine real-world breach cases to understand how human behavior impacts cybersecurity.
- Identify accountability gaps and reinforce personal responsibility in safeguarding client data.
- Apply best practices to strengthen the human layer as the bank's first line of defense.

5. Closing & Business Application

- Consolidate key takeaways into actionable cybersecurity habits for daily banking practice.
- Commit to one behavior change that enhances data protection and client trust.
- Reinforce accountability and sustain a culture of digital vigilance across teams.

PRACTICE & APPLICATION

- Investigate real-world cybersecurity breach cases and identify what went wrong.
- Collaborate in teams to assess threats, human errors, and preventive measures.
- Practice client-facing conversations to explain data-protection best practices in simple, trusted language.
- Reflect on lessons learned and commit to only cyber-safe behavior for immediate application.

KEY VALUE PROPOSITION

- Translates complex cybersecurity and data-privacy standards into clear, practical actions for bankers.
- Builds awareness and accountability to reduce human-error risks in daily operations.
- Strengthens client trust through secure practices and confident communication on data protection.

About IBF Certification

Participants are encouraged to access the IBF MySkills Portfolio (https://www.ibf.org.sg/home/for-individuals/resource-tools/myskills-portfolio) to track their training progress and skills acquisition against the Skills Framework for Financial Services. You can apply for IBF Certification after fulfilling the required number of Technical Skills and Competencies (TSCs) for the selected job role. Find out more about IBF certification and the application process on here.

Up to 70% Funding*

for Singaporeans and PRs

Terms & Conditions apply

Funding:
IBF Standards training Scheme (IBF-STS)

www.momenta.biz

Penny Tang: +65 9003 2890 | penny.tang@momenta.biz