BLACKBIRD FOR TRAINING

Security Awareness: Protecting ATM Operations and Financial Data from Modern Security Threats

15 – 19 February 2027
London (UK)

UK Traininig
PARTNER



www.blackbird-training.com

Security Awareness: Protecting ATM Operations and Financial Data from Modern Security Threats

Ref: 3255851_353791 **Date:** 15 – 19 February 2027 **Location:** London (UK) **Fees:** 6100 GBP

Introduction

Security Awareness has become a critical component of organizational resilience, particularly in environments that rely on financial systems, digital infrastructure, and customer-facing technologies such as Automated Teller Machines. As cyber threats continue to evolve, organizations must ensure that employees, operators, technicians, and information security personnel understand how to recognize, prevent, and respond to security risks that could compromise data, operations, and customer trust.

This course provides participants with a practical understanding of security threats affecting ATM environments and financial operations. It focuses on developing the knowledge required to identify suspicious activities, recognize indicators of fraud, protect sensitive information, and support incident response processes. The program emphasizes the human element of security and the role employees play in maintaining a secure operational environment.

Participants will explore threats such as card skimming, unauthorized access, data breaches, social engineering attacks, and operational security weaknesses. The course also covers data protection principles, encryption requirements, access control mechanisms, incident reporting procedures, and security compliance responsibilities.

Through practical examples, real-world case studies, and interactive discussions, participants will strengthen their ability to identify security risks, support organizational security initiatives, and contribute to a stronger security culture within their institutions.

Course Objectives

By the end of this course, participants will be able to:



- Understand the principles and importance of Security Awareness.
- Identify common security threats affecting financial operations.
- Recognize indicators of card skimming and fraud attempts.
- Understand how cyber threats impact ATM environments.
- Apply data protection and information security practices.
- Understand the role of encryption in securing sensitive data.
- Implement secure access and authentication practices.
- Support incident response and reporting procedures.
- Identify suspicious activities and security anomalies.
- Reduce operational risks through security best practices.
- Support compliance with organizational security policies.
- Improve awareness of information security responsibilities.
- Contribute to a stronger security culture within the workplace.
- Participate effectively in security risk mitigation activities.
- Enhance overall operational security awareness.

Course Outlines

Day 1: Foundations of Security Awareness and Risk Management

- Understanding Security Awareness and its organizational importance.
- Current threat landscape and emerging security risks.
- Information security principles and objectives.
- Roles and responsibilities in maintaining security.
- Operational security risks in financial environments.
- Security best practices for daily operations.
- Identifying vulnerabilities and potential threats.
- Practical exercises on risk recognition and assessment.

Day 2: ATM Security Threats and Fraud Prevention

- Overview of ATM-related security threats.
- Understanding card skimming techniques and methods.
- Indicators of tampering and unauthorized device installation.
- Physical security threats affecting ATM operations.
- Unauthorized access risks and prevention measures.
- Fraud detection and prevention strategies.
- Security monitoring and early threat identification.
- Case studies involving ATM security incidents.



Day 3: Data Protection and Encryption Fundamentals

- Importance of protecting sensitive financial information.
- Data classification and handling requirements.
- Fundamentals of encryption and secure communications.
- Protecting customer and transaction data.
- Access management and authentication controls.
- Password security and credential protection.
- Securing data during transmission and storage.
- Practical exercises on data protection practices.

Day 4: Security Incident Response and Investigation

- Understanding security incidents and their impact.
- Incident response lifecycle and procedures.
- Security reporting and escalation processes.
- Initial evidence collection and documentation.
- Incident containment and mitigation techniques.
- Communication during security events.
- Preparing incident reports and records.
- Practical incident response scenarios.

Day 5: Security Compliance and Building a Security Culture

- Security compliance requirements and obligations.
- Organizational security policies and procedures.
- Security audits and continuous monitoring.
- Measuring the effectiveness of security awareness initiatives.
- Developing a strong organizational security culture.
- Continuous improvement of security controls.
- Integrated case study covering threats, protection, and response.
- Final assessment and review of key security concepts.

Why Attend This Course: Wins & Losses!

- Improve the ability to recognize security threats.
- Strengthen protection of sensitive information and data.
- Enhance awareness of operational and cybersecurity risks.
- Develop skills for identifying card skimming activities.
- Improve incident reporting and response capabilities.
- Support compliance with security policies and standards.
- Strengthen organizational security culture.
- Reduce exposure to fraud and information security threats.
- Improve collaboration between operational and security teams.
- Increase overall security readiness across the organization.



Conclusion

Security Awareness is one of the most effective defenses against modern security threats. While organizations continue to invest in advanced security technologies, the human factor remains a critical component in preventing incidents, detecting suspicious activities, and supporting secure operations. Employees who understand security risks are better equipped to protect organizational assets, customer information, and business continuity.

This course provides a comprehensive understanding of security threats affecting ATM environments and financial operations, including card skimming, data protection challenges, encryption requirements, access management controls, and incident response procedures. Participants gain practical knowledge that helps them recognize risks and take appropriate actions to reduce security vulnerabilities.

The program also emphasizes the importance of security culture, compliance, and continuous awareness. By combining technical concepts with operational practices and real-world examples, the course helps participants strengthen their ability to contribute to a safer and more resilient working environment.

Upon completion, participants will be better prepared to identify threats, support security initiatives, protect sensitive information, and respond effectively to security incidents, helping their organizations maintain trust, compliance, and operational stability.

