CYBERSECURITY · SHORT COURSE

Cybersecurity for HR Teams – Protecting Employee Data & Privacy

Human Resource (HR) departments manage some of the most sensitive organizational data, including:

DATES	11–15 Jan 2027	DURATION	5-day course
COURSE FEE	TZS 1,300,000 · per participant	VAT	Fee excludes VAT
VENUE	Arusha, Tanzania	DAILY HOURS	8:30 AM – 4:30 PM
FEE INCLUDES	Course materials, lunch and refreshments	CERTIFICATE	Certificate of attendance
TRAINER	Elly International training team	APPLICATIONS	Open for applications

Overview

Human Resource (HR) departments manage some of the most sensitive organizational data, including:

- Personal identification information
- Payroll and salary records
- Medical and benefits data
- Disciplinary records
- Employment contracts
- Performance evaluations

Because of the sensitive nature of this data, HR units are increasingly targeted by:

- Phishing and social engineering attacks
- Payroll fraud schemes
- Business Email Compromise (BEC)
- Insider threats
- Data leakage incidents
- Unauthorized access to employee records

Many HR teams, however, lack structured cybersecurity awareness and practical safeguards tailored to HR operations. Common weaknesses include:

- Weak password and access management practices
- Poor handling of confidential documents
- Overexposed shared drives and email attachments
- Limited understanding of data protection regulations
- Lack of incident response preparedness

There is therefore a strong need for a practical, HR-focused cybersecurity course that equips HR professionals with the knowledge and tools to securely manage employee data, reduce risk exposure, and respond effectively to security incidents.

Course content

Day 1: Cyber Threat Landscape & HR Risk Exposure

Module 1: Cybersecurity Fundamentals for HR

- Basic cybersecurity concepts
- Why HR is a high-value target
- Types of cyber threats affecting HR

Module 2: Phishing & Social Engineering

- Email phishing techniques
- Payroll redirection scams
- CEO fraud and impersonation attacks
- Safe verification procedures

Practical Session (Hands-On)

- Identifying phishing emails
- Simulated HR fraud scenarios
- Risk mapping for HR functions

Day 2: Protecting Employee Data & Privacy

Module 3: Data Classification & Secure Handling

- Types of employee data
- Data sensitivity levels
- Secure storage and transmission
- Encryption basics

Module 4: Access Control & Password Management

- Role-based access control
- Least privilege principle
- Multi-factor authentication (MFA)
- Secure shared folder practices

Practical Session (Hands-On)

- Reviewing access control scenarios
- Identifying overexposed HR files
- Designing a simple data classification guide

Day 3: Secure Communication & Insider Risk Management

Module 5: Secure Email & Document Sharing

- Safe attachment handling
- Secure cloud storage practices
- Protecting payroll data
- Avoiding data leakage

Module 6: Insider Risk & Data Leakage Prevention

- Types of insider threats
- Monitoring and audit basics
- Exit process security controls
- HR’s role in reducing insider risk

Practical Session (Hands-On)

- Insider risk case studies
- Designing secure exit procedures
- Reviewing document handling workflows

Day 4: Compliance, Privacy & Incident Response

Module 7: Data Protection & Regulatory Compliance

- Principles of data protection
- Privacy obligations
- Employee consent and lawful processing
- Record retention policies

Module 8: HR Incident Response Readiness

- Recognizing a data breach
- Immediate response steps
- Reporting and escalation
- Communication during incidents

Practical Session (Hands-On Labs)

- Simulated data breach exercise
- Drafting an HR incident response checklist
- Privacy compliance gap assessment

Day 5: Strengthening HR Security Governance & Capstone

Module 9: HR Security Governance

- Policy development basics
- Secure onboarding procedures
- Secure offboarding procedures
- Documentation and audit preparation

Module 10: Building a Secure HR Environment

- Risk assessment basics
- Continuous improvement strategies
- Staff awareness and training
- Collaboration with ICT/security teams

Capstone Practical Simulation
Participants will complete an HR cybersecurity improvement project, including:

- HR risk assessment
- Data protection improvement plan
- Incident readiness checklist
- Access control review
- Policy enhancement recommendations

Course Wrap-Up

- Practical evaluation
- Participant reflections
- Facilitator recommendations
- Certificate guidance

Who should attend

Target Group

This course is suitable for:

- HR Officers
- HR Managers
- Compliance Officers
- Records and Documentation Officers
- Payroll Teams
- Administrative Officers
- Employee Relations Officers

- HR Business Partners

Recommended Prerequisites

- Basic computer literacy
- Familiarity with HR operations
- No technical cybersecurity background required

How to apply

Apply online at ellyinternational.co.tz. Your place is confirmed only after we review your application and contact you, within 1 working day.

Apply for this course | **Ask on WhatsApp** | **Email us**

+255 757 066 880 · training@ellyinternational.co.tz · Boma Road, Arusha, Tanzania · P.O. Box 13424
Details correct as of 28 November 2026.