



OXFORD
COLLEGE OF MANAGEMENT

Cybersecurity Risk Points in HR Processes

Recruitment:

- Online Job Portals: Secure handling of job postings and application submissions.
- Resume Submission: Protection of personal information provided by candidates.
- Background Checks: Secure data exchange during background verification processes.
- Communication: Ensuring secure emails and online communications with candidates.

Onboarding:

- Data Collection: Secure storage of personal employee data.
- System Access: Safeguarded setup of access to company systems for new hires.
- Hardware and Software: Controlled distribution of company technology.
- Benefits Enrolment: Secure handling of sensitive information related to health and benefits programs.

Data Management:

- Employee Details Storage: Securing personal details such as addresses and financial information.
- Access Controls: Robust controls over sensitive HR databases.
- Data Transfer: Secure regular data transfers within and outside the organisation.
- Cloud and Third-party Processors: Ensuring the security of cloud storage and third-party data handling.

Employee Management:

- Record Updates: Secured processes for regularly updating employee records.
- Performance Data: Secure handling of performance evaluations and feedback.
- Grievances and Disciplinary Records: Privacy and security in managing sensitive records.

Payroll and Benefits Administration:

- Payroll Systems: Secure access to systems processing payroll and bank details.
- Benefits Management: Securing data related to health insurance and pension plans.
- Third-party Confidentiality: Ensuring third-party service providers protect confidential data.

Third-party Interactions:

- **External Consultants:** Secure interactions with external HR services.
- **Outsourced Functions:** Protection of data in outsourced payroll or benefits administration.
- **External Recruiters:** Secure data exchange with recruiters and staffing agencies.

Technology and System Access:

- **HR Software:** Secure use of HR management databases and software.
- **Remote Access:** Security measures for remote access to HR systems.
- **Mobile Device Security:** Ensuring the security of mobile devices and laptops used in HR operations.

Compliance and Legal:

- **Data Protection Laws:** Compliance with laws like GDPR and HIPAA.
- **Consent Forms:** Secure handling of employee consent and privacy notices.
- **Legal Disclosures:** Controlled disclosures of employee information.

Offboarding:

- **Access Deactivation:** Proper deactivation of access rights upon employee departure.
- **Data Disposal:** Secure disposal of personal data post-employment.
- **Final Transmissions:** Safe transmission of final payroll and benefits information.

Training and Awareness:

- **Cybersecurity Training:** Regular training sessions for HR staff on cybersecurity.
- **Phishing Awareness:** Educating about social engineering threats like phishing.
- **Training Updates:** Continuous updates to training materials with current security practices.

Incident Management:

- **Breach Detection:** Efficient detection and response to data breaches.
- **Reporting Channels:** Established channels for reporting suspicious activities.
- **Recovery Processes:** Robust recovery and backup procedures for HR data.