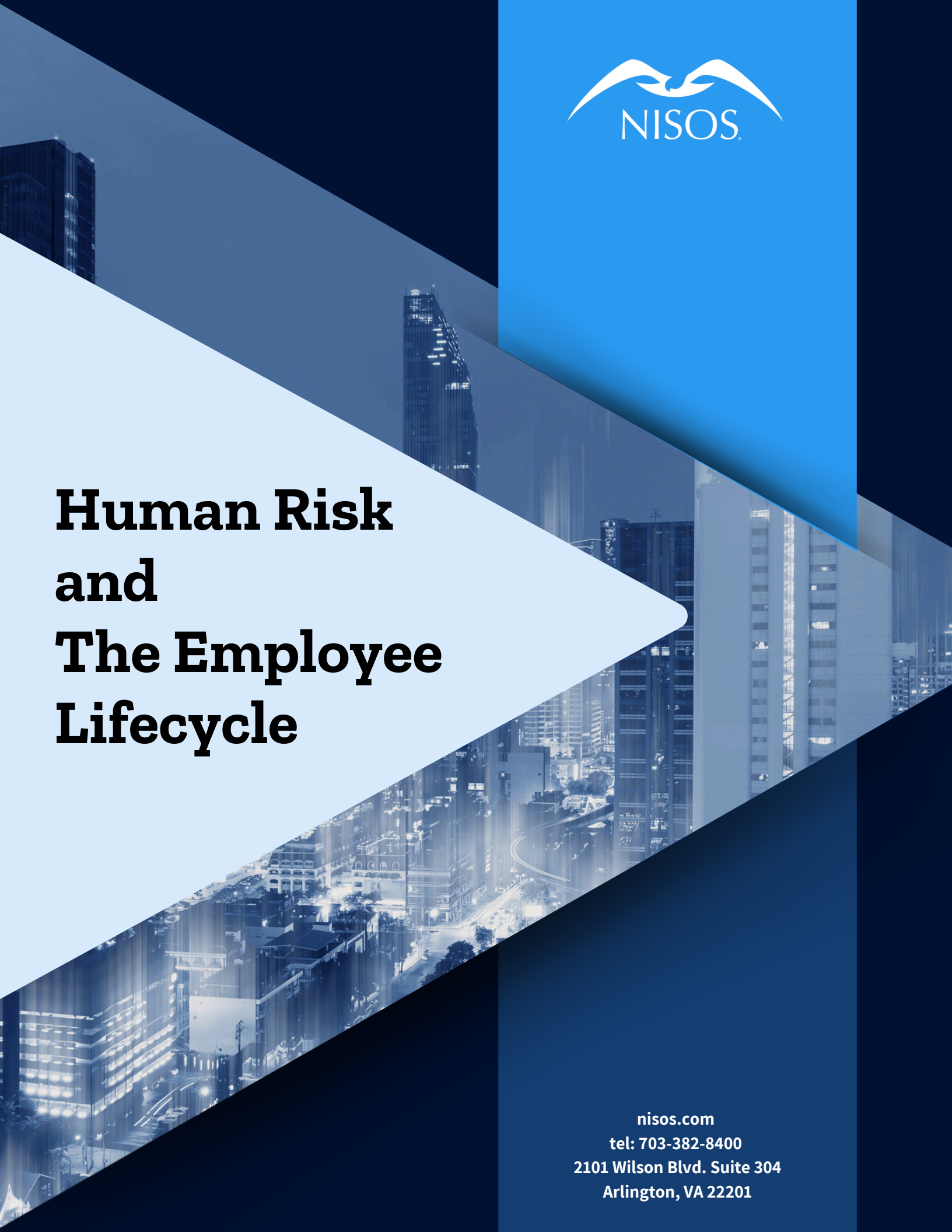


Human Risk and The Employee Lifecycle

nisos.com
tel: 703-382-8400
2101 Wilson Blvd. Suite 304
Arlington, VA 22201

Executive Summary

Human Resources (HR) plays a critical role in identifying and mitigating human risks throughout the Employee Lifecycle (ELC). By addressing employment fraud such as falsified credentials, insider threats, and data security beaches, HR professionals can proactively protect their organizations. Partnering with security teams enables HR to implement robust processes, enhance employee training, and safeguard sensitive data, ensuring the company can mitigate evolving human threats.

Stages of the ELC

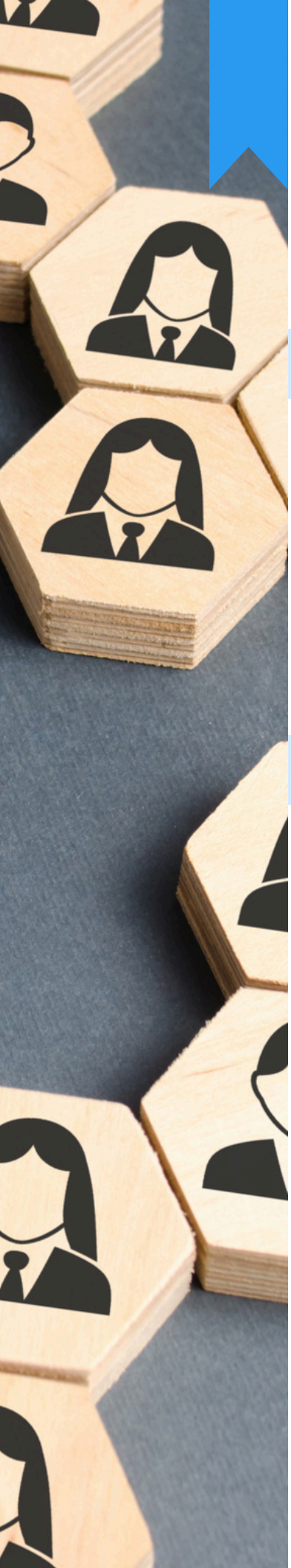
Recruitment
Create awareness of the company among potential candidates and establish a brand that attracts a diverse array of top candidates. Ensure an efficient, consistent and equitable process that effectively screens and selects a diverse array of high potential team members who embody the company's core values.

Onboarding
Provide the knowledge, resources, and support for new hires to make an accelerated contribution while positively reinforcing their decision to join the company.

Engagement
Create an environment where team members are inspired by, enabled to execute on, and aligned with our mission and goals, and feel highly satisfied with their work at the company.

Learning & Development
Support the employee to achieve their full potential through training, performance management, professional development, and advancement opportunities.

Offboarding
Professionally and respectfully transition the departing employee in a manner that supports both ongoing company operations and the employee's journey to their next opportunity.



Stage 1: Recruitment

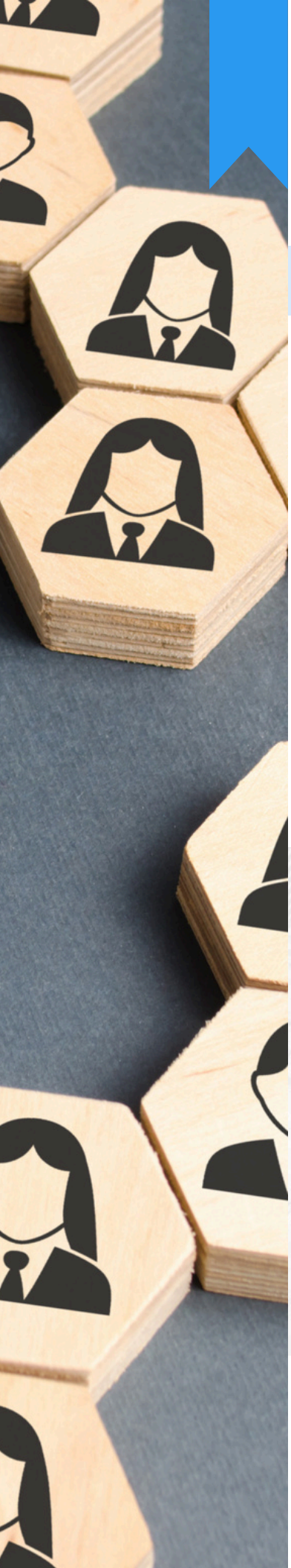
Recruitment is the first stage in the ELC, and while it offers the opportunity to identify top talent, it also introduces risks that can threaten an organization's security.

Key Risks:

- Candidates may falsify their credentials or misrepresent their qualifications, creating vulnerabilities in critical roles.
- Hiring teams may unintentionally reveal confidential company information during the interview process.
- Inadequate background checks could fail to identify high-risk individuals, such as individuals engaged in polywork (individuals working multiple jobs at the same time) or individuals who are aligned with interests that conflict with the organization's values.

HR Solutions:

- Treat applicant data as highly sensitive information. Secure candidate data by using an Applicant Tracking System (ATS) with encryption and access controls to protect sensitive candidate data.
- Use an ATS with machine learning or other automated tools that can flag inconsistencies and patterns of falsification, such as different names used on the same resume, different names used between the resume and the application, etc.
- Train recruiters and hiring teams to look for anomalies between the resume and the interview.
- Require all candidates to participate in a video interview or an in-person interview to confirm identity and assess non-verbal communication.
- Train hiring teams to avoid disclosing proprietary information and instead focus on behavioral and situational interview techniques. Consider providing final candidates a non-disclosure agreement if you plan to share proprietary information.
- Develop robust background checks policies that assess criminal records, credit histories, and provide employment verifications, education verifications and social media checks.



Stage 1: Recruitment

Security Partnership:

- Work with the security team to define acceptable risk thresholds for critical positions (e.g. history of bankruptcy for roles managing financial systems, moonlighting work that is in direct conflict with the organization's interest, ties to competitors for leadership roles, frequent travel to locations known for corporate espionage, publicly promoting views that do not align with the company and could damage the company's brand or reputation).
- Integrate security personnel into the recruitment process to flag risks.
- Engage the security team to vet the candidate's digital footprint by analyzing publicly available information on candidates, including social media.
- Use technology to verify the candidate's physical location during the interview (if virtual). This could be checking IP addresses, requiring geo-tagged video calls, or confirming local knowledge through conversation.

Case Study

Falsified credentials led to to a security breach (KnowBe4 incident)

In mid July 2024, a US security awareness training company revealed that it unwittingly hired a North Korean hacker using a stolen identity for a remote Principal Software Engineer position. This example of a successful employment fraud is one of many in which the Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) information technology (IT) workers successfully used fake personas and stolen identities of American citizens to fraudulently obtain remote employment from unwitting companies in the United States.

Link >>>

Stage 1: Recruitment

Recruitment Checklist:

Step	Action	Responsibility	Completed (✓)
Pre-screening	Verify resume and credentials (e.g. education, certifications)	HR	
Background Check	Conduct criminal check, SSN check, sex offender registry, credit report, etc.	HR	
Digital Risk Review	Partner with a background check company to assess the candidate's digital footprint.	HR	
Data Handling	Secure candidate data in an encrypted ATS.	IT/HR	
Final Review	Evaluate candidate risk profile with HR, Security, and the hiring manager.	HR/CISO/Manager	

Stage 2: Onboarding

Onboarding is a pivotal phase where employees gain access to critical systems and sensitive information. If mishandled, it can open doors to human risk.

Key Risks:

- Employees granted excessive access during onboarding may inadvertently expose data or misuse systems.
- Employees who are not provisioned equipment or access in a timely manner may use their personal devices which may lack proper security controls and therefore increase the likelihood of sensitive data being exposed.
- Lack of immediate awareness about security policies and practices increases vulnerability.

HR Solutions:

- Conduct in-person orientations or require that cameras are turned on for virtual sessions to validate authenticity of the employee.
- Ensure employees are using company-issued devices and accessing the company's network.
- Include security awareness training in the first week, covering phishing attacks, password protocols, and data protection best practices.
- Collaborate with IT to implement role-based access controls, ensuring employees only access systems relevant to their job functions.
- Assign distinct identifiers or prefixes to system profiles based on the role (e.g. CON- for contractors, VEN- for vendors).
- Automate user provisioning and deprovisioning to ensure consistency and reduce the risk of errors

Security Partnership:

- Develop onboarding materials and training in partnership with security.
- Automate provisioning and deprovisioning of access through identity management tools.
- Schedule joint HR and Security check-ins to address onboarding anomalies or concerns.

Stage 2: Onboarding

Case Study

Data Breach Impacts Thousands of NHS Workers

Around 14,000 employees at a Liverpool NHS hospital trust were notified that their data was accidentally leaked through email. A file containing sensitive payroll information was sent to multiple NHS managers and 24 external accounts. The file had a hidden tab with personal details, including names, addresses, dates of birth, National Insurance numbers, gender, ethnicity, and salary, though it did not contain bank account information.

Link >>>

Onboarding Access Checklist

Step	Action	Responsibility	Completed (✓)
Provision equipment	Provide the employee with a company laptop, access cards, etc.	IT	
Provision Access	Assign system access based on role and responsibilities. Enable multi-factor authentication (MFA) for all accounts.	IT	
Security Training	Deliver mandatory security awareness training (e.g. phishing, data handling.) Confirm completion of training within 30 days	IT/HR	
Policy Acknowledgement	Have employees sign acknowledgement of IT security and data handling policies.	HR	
Access Audit	Verify access levels match roles after the first 60 days.	IT	

Stage 3: Engagement

Employee engagement plays a vital role in shaping an organization's culture, productivity, and overall morale. However, disengaged employees do not just underperform—they can become disgruntled and become significant insider threats.

Key Risks:

- Lack of motivation or dissatisfaction can lead to malicious or negligent behavior.

HR Solutions:

- Set and regularly review clear performance expectations and objectives with employees.
- Strengthen engagement through recognition programs and frequent feedback.
- Create opportunities for team bonding, especially for remote and hybrid workers.
- Offer robust career development programs and clearly communicate growth pathways.
- Identify early warning signs of discontent through surveys and pulse checks.
- Implement tools to monitor engagement and data use to detect insider threats.
- Train managers to identify and address conflicts or toxic behavior early.

Security Partnership:

- Share insights from engagement surveys with security teams to identify potential risks.
- Collaborate on training programs that blend engagement with security awareness.
- Partner with the security team to monitor online engagement and behavior anomalies such as employees accessing unusual websites or platforms unrelated to their job functions, employees logging in or accessing sensitive systems at times that are inconsistent with their normal work pattern, unusual file transfers, sudden activity on professional competitor forums, excessive downloading or other actions that deviate from the employee's typical patterns.

Stage 3: Engagement

Case Study

Yahoo Lawsuit Accuses Former Scientist of Stealing IP for Competitor

Yahoo has alleged its former research scientist, Qian Sang, had stolen intellectual property in February 2022. The company claims that Sang intended to use the stolen data for financial gain with Yahoo's competitor, The Trade Desk, after receiving a job offer from them. In addition to intellectual property, Sang allegedly took confidential documents, including Yahoo's strategic plans and competitive analysis of The Trade Desk. He reportedly transferred the data from his work laptop to two personal external storage devices.

Link >>>

Engagement Pulse Survey

Question
How satisfied are you with your role?
Do you feel your work is valued?
Do you feel comfortable reporting concerns to your manager?
What changes could improve your experience at work?

Stage 4: Learning & Development

Learning and development programs empower employees but also expose the organization to risks if knowledge or skills are misused. Conversely, when training doesn't happen, employees may lack the skills needed for the job function and could lead to inadvertent release of sensitive data or failure to adhere to critical security controls.

Key Risks:

- Learning and Development platforms may be vulnerable to breaches, exposing employee and organizational data.
- Without target training for specific roles, employees may inadvertently mishandle sensitive data.
- Employees who are not trained in ethical behavior and responsible use of acquired skills may unintentionally engage in harmful actions.

HR Solutions:

- Conduct regular security awareness training.
- Incorporate discussions about ethical behavior and responsibility into technical and leadership training.
- Ensure employees receive training tailored to their roles that emphasizes handling sensitive information appropriately (e.g. phishing for marketing, data protection for finance, safeguarding personal employee data, securing code to avoid vulnerabilities).
- Ensure the Learning and Development platform adheres to regulatory and data protection standards. Ensure it has strong encryption, secure APIs, access controls, and does not have a history of breaches.

Security Partnership:

- Partner with security and IT to audit learning and development platforms for vulnerabilities. Use platforms that prioritize encryption and role-based access.
- Collaborate with security to design role-specific security training.
- Establish a feedback mechanism to evaluate training outcomes to ensure employees demonstrate understanding and compliance.
- Partner with security teams to integrate scenarios and case studies into training that focus on ethical behavior and responsible use of advanced skills, reinforcing a culture of integrity.

Stage 4: Learning & Development

Case Study

Ex-Ubiquiti Employee Pleads Guilty to Stealing Data and Extorting the Company

Nickolas Sharp, a former Ubiquiti employee who led the company's cloud team, pleaded guilty to stealing gigabytes of files from Ubiquiti's network and attempting to extort the company. Posing as an anonymous hacker and whistleblower, Sharp demanded a ransom, and when his demands were not met, he orchestrated false news stories about Ubiquiti. These actions caused the company's market value to drop by over $4 billion.

Link >>>

Learning and Development Security Training Topics

Role/Department	Training Topics	Completion Deadline
Marketing/HR	Phishing awareness, social engineering risks, safe social media use.	30 days post-onboarding
Finance/HR	Data protection, regulatory compliance, secure transaction handling.	30 days post-onboarding
IT/Security	Advanced cybersecurity protocols, incident response.	Ongoing
Engineering/Technology	Responsible use and ethical behavior	Ongoing
Executive Leadership	High-risk insider threats, credential theft prevention.	Ongoing

Stage 5: Offboarding

The offboarding process is critical to prevent data leaks, mitigate insider threats, and maintain a positive employer brand.

Key Risks:

- Failure to revoke access to systems can lead to breaches.
- Disgruntled employees may steal or destroy data.

HR Solutions:

- Develop a standardized process that includes access revocation, equipment return, and final settlements.
- Identify unresolved grievances or risks through well-designed exit interviews.
- Remind employees of their obligations under their confidentiality agreement (if applicable).
- Train your teams to ensure they know the roles they play and their responsibilities during offboarding.
- Conduct exit interviews that include questions about the employee's access and use of company systems to identify any gaps in deprovisioning or potential risks.

Security Partnership:

- Establish heightened monitoring for high-risk employees such as those in privileged roles or with access to sensitive data, to detect any unusual behavior during the notice period.
- Partner with security and IT to ensure immediate deprovisioning of accounts and accesses.
- Consider automating workflows and incorporating technology solutions to ensure consistency, efficiency and to reduce human error.
- Review and audit the departing employee's data access logs for unusual activity, such as large file downloads, email forwarding, or external device usage.
- For employees in sensitive roles, consider limiting access to critical systems during their notice period to mitigate risks.

Stage 5: Offboarding

Case Study

Former Cash App Employee Potentially Exposes Personal Data of 8 Million Users

A data breach potentially affected over 8 million Cash App users after a former employee downloaded reports containing sensitive personal data. While the ex-employee had access to the data during their employment, the download occurred after they left the company. The breached data includes full names, brokerage account numbers, and details of stock activity on Cash App Investing, but does not contain usernames, passwords, Social Security numbers, or bank account information. Additional exposed information included brokerage portfolio value, holdings, and trading activity for one trading day.

Link >>>

Offboarding Checklist

Step	Action	Responsibility	Completed (✓)
Access Revocation	Disable employee access to all systems and platforms immediately.	IT	
Equipment Return	Retrieve company-owned devices (laptops, phones, etc.)	IT/HR	
Exit Interview	Conduct an exit interview to identify unresolved grievances or risks.	HR	
Final Settlements	Process final payments and benefits.	HR	

Conclusion

HR professionals are essential in safeguarding organizations from a wide range of human risks throughout the ELC. By addressing vulnerabilities that can occur from recruitment through offboarding, HR can prevent potential fraud, insider threats, and data breaches. Through close collaboration with security teams, HR can implement strong processes, training, and tools to ensure that sensitive information is protected, and risks are minimized.

As the workforce evolves, HR's role in safeguarding an organization against human risk will only become more critical. Protecting an organization is a shared responsibility, and HR professionals must remain vigilant in identifying and mitigating potential threats at every stage. By actively engaging with security teams and prioritizing proactive risk management, HR can play a pivotal role in maintaining both the security and integrity of their company, ultimately ensuring a safe, productive, and ethical work environment. By doing so, HR can protect the organization's assets, enhance its reputation, and contribute to long-term success.

About Nisos®
Nisos is a trusted digital investigations partner specializing in unmasking human risk. We operate as an extension of security, risk, legal, people strategy, and trust and safety teams to protect their people and their business. Our open source intelligence services help enterprise teams mitigate risk, make critical decisions, and impose real world consequences.

For more information visit:
www.nisos.com
email: info@nisos.com
call: +1-703-382-8400
follow: LinkedIn