KnowBe4

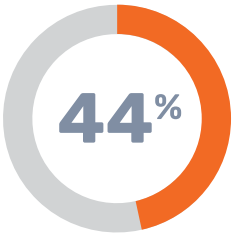
# AI-Driven Scams and Fraudulent CVs: The Increased Risk to HR Operations in the UK

## Introduction

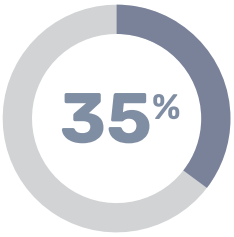
A recent survey of 1,001 HR professionals in organisations with over 100 employees reveals significant challenges related to cybersecurity and the growing use of AI in recruitment processes. This survey report delves into the latest cybersecurity challenges faced by HR professionals, highlighting the surge in AI-driven fraud, the gaps in cybersecurity awareness, and the pressing need for improved collaboration between HR and IT departments.

## Fraudulent Job Applications

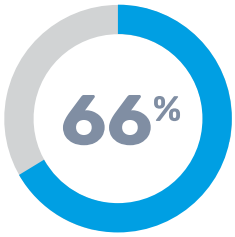
The prevalence of fraudulent job applications presents a big challenge for HR professionals, with 44% encountering such applications. More alarmingly, over a third of these fraudulent applications contained cybersecurity threats in the form of malicious links or attachments, highlighting the evolving risks in the recruitment process.



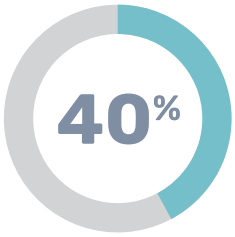

**HR professionals have encountered fraudulent or scam job applications**




**Fraudulent CVs contained malicious links or attachments**



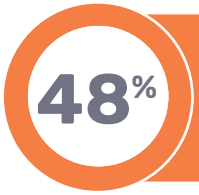

**Identified CVs generated by AI, with a significant portion being fraudulent**




**HR professionals admitted progressing a job application before realising fraud**

## Use of AI in Recruitment

The adoption of artificial intelligence in human resources is gaining momentum, transforming traditional recruitment processes. A significant 37% of HR teams are already utilising AI tools to streamline the screening of job applications, while 29% employ AI technology to craft job specifications. This trend towards AI integration is further emphasised by the growing interest in fraud detection, with 37% of HR professionals advocating for AI-based tools to identify fraudulent applications.



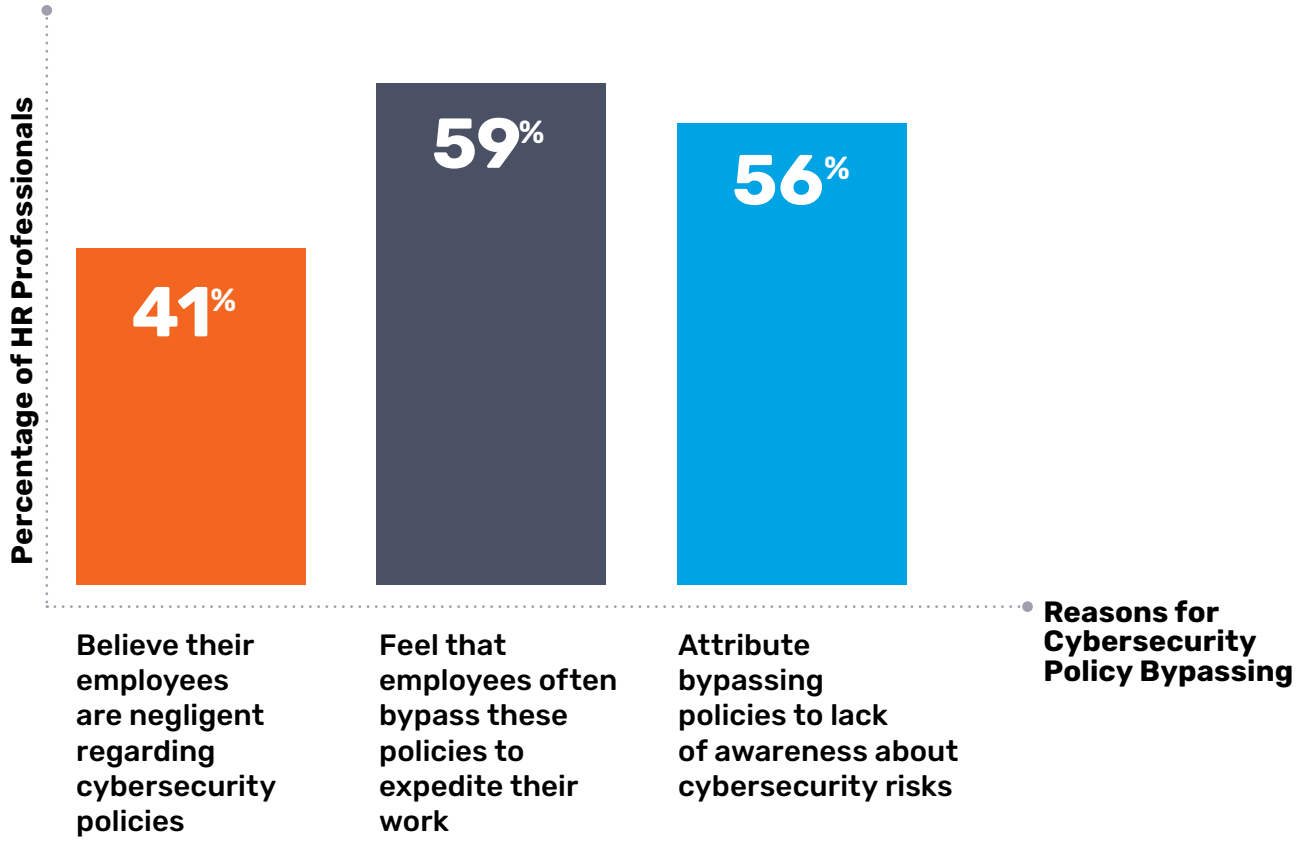

**HR professionals have interacted with Linkedin profiles that were later found to be fake.**

## Cybersecurity Awareness and Compliance

Employee adherence to cybersecurity policies remains a significant challenge for organisations, with HR professionals expressing concern over widespread negligence in this area. More distressing is that there's a perception that employees frequently bypass these policies to accelerate their work processes, often due to a lack of awareness about cybersecurity risks.

While organisations are implementing various training programmes to address these concerns, the persistence of policy breaches suggests that current approaches may be insufficient. This situation highlights a critical gap between the implementation of cybersecurity measures and employee compliance, underscoring the need for more effective and engaging awareness programmes.

To foster a robust cybersecurity culture, organisations may need to reevaluate their training methods and consider different approaches that resonate more with employees and their day-to-day work practices.




Despite these issues, 40% of organisations conduct cybersecurity awareness training quarterly, while 19% do it annually, and 16% at intervals longer than quarterly but shorter than bi-annually.

## Incidents and Vulnerabilities

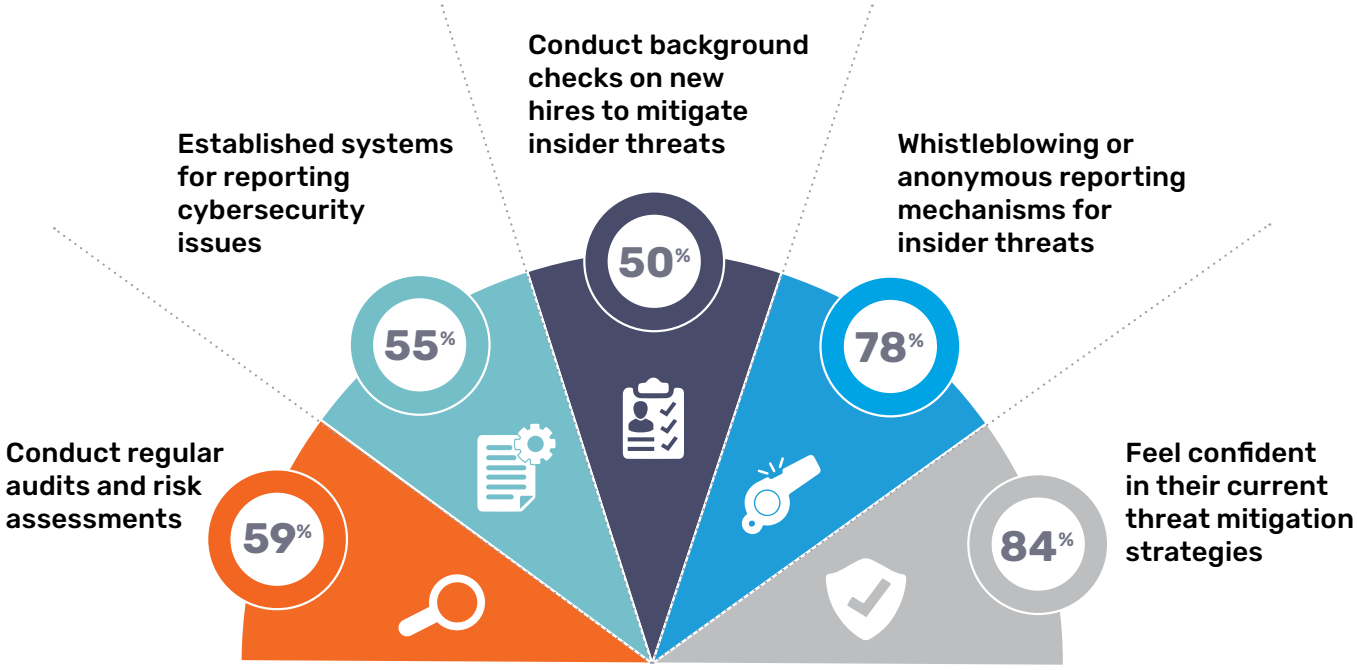
Over half (57%) of respondents reported their organisations have fallen victim to phishing-related cyberattacks in the past year. Data breaches remain a concern with 35% reporting unauthorised access to sensitive information and 31% experiencing data leaks or theft. The situation is particularly worrying for HR professionals, where 82% have faced a cybersecurity incident over the last 12 months. Despite this high incidence rate, 40% of organisations lack a formal incident response plan, emphasising a critical gap in preparedness against cyber threats.

## Current Mitigation and Reporting Strategies

In the face of growing cybersecurity challenges, organisations are implementing a range of measures to strengthen their defences. Many are taking proactive steps, conducting regular audits and risk assessments to identify vulnerabilities in their systems. Establishing formal channels for reporting cybersecurity issues is also becoming more common, facilitating early detection and response to potential threats.

To mitigate insider risks, a large number of organisations have incorporated background checks into their hiring processes, aiming to screen out potential security liabilities before they enter the workforce. The widespread adoption of whistleblowing and anonymous reporting mechanisms further demonstrates a commitment to creating a culture of security awareness and accountability.

However, the high level of confidence expressed by many organisations in their threat mitigation strategies may be misplaced, given the prevalence of reported cybersecurity incidents. This disconnect suggests a potential blind spot in organisational self-assessment, pointing out the need for more rigorous and frequent evaluation of cybersecurity measures. It is crucial for organisations to maintain a realistic view of their security posture and continually adapt their strategies to address evolving threats in the digital landscape.




## Collaboration and Training Needs

The evolving landscape of cybersecurity threats has highlighted the need for a more integrated approach to online security. More than half of respondents (52%) are calling for closer partnerships with IT and security teams, reflecting a growing recognition that effective cybersecurity is not solely the domain of IT, but requires input and vigilance from all departments in an organisation.

Simultaneously, 44% of HR professionals are demanding more specialised training for HR and recruitment teams, focusing on the identification and mitigation of security risks. This highlights the increasing complexity of cybersecurity challenges in the hiring process and daily operations, and acknowledges the critical role that HR plays in maintaining an organisation's security posture.

**44%** HR professionals demand more specialised training for HR and recruitment teams.

By fostering these interdepartmental relationships and enhancing skill sets, organisations can create a stronger and more responsive security culture that is better equipped to face the challenges of the digital age. These statistics clearly demonstrate a shift towards a more collaborative and educated approach to cybersecurity within the HR function.

## Recommendations

- **Enhance Cybersecurity Training:** Given the rise in AI-generated fraud and phishing incidents, organisations should prioritise more frequent and targeted cybersecurity training for all employees, especially HR and recruitment teams.
- **Invest in AI Detection Tools:** As AI-generated applications become more prevalent, adopting AI-based detection tools could help identify and mitigate fraud early in the recruitment process.
- **Strengthen Incident Response Plans:** With a significant portion of organisations lacking incident response plans, it's critical to establish and regularly update these protocols to minimise damage from cyber incidents.
- **Boost Cross-Department Collaboration:** Facilitating stronger collaboration between HR, IT, and security teams can improve the organisation's overall cybersecurity posture and enhance threat detection capabilities.

The survey report highlights the urgent need for HR departments to not only protect their own processes from cyber threats but also to serve as a frontline defence against the increasing sophistication of cyberattacks targeting recruitment channels. By addressing these gaps through training, technology, and interdepartmental collaboration, organisations can better safeguard their data and systems against AI driven cyber threats and strengthen the organisation's overall security culture.

## Additional Resources

**Free Phishing Security Test**
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

**Free Automated Security Awareness Program**
Create a customized Security Awareness Program for your organization

**Free Phish Alert Button**
Your employees now have a safe way to report phishing attacks with one click

**Free Email Exposure Check**
Find out which of your users emails are exposed before the bad guys do

**Free Domain Spoof Test**
Find out if hackers can spoof an email address of your own domain


## About KnowBe4

KnowBe4 empowers your workforce to make smarter security decisions every day. Tens of thousands of organizations worldwide trust the KnowBe4 platform to strengthen their security culture and reduce human risk. KnowBe4 builds a human layer of defense so organizations can fortify user behavior with new-school security awareness and compliance training.

Deploying KnowBe4 results in users that are alert and care about the damage that phishing, ransomware and other social engineering threats pose. The platform includes a comprehensive suite of awareness and compliance training, real-time user coaching, AI-powered simulated social engineering, and crowdsourced anti-phishing defense.

With content in 35+ languages, KnowBe4 provides the world's largest, always-fresh library of engaging content to strengthen your human firewall.

**For more information, please visit www.KnowBe4.com**

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com



01E12K01