PHISHING T@CKLE

From Tick-Box to Boardroom: The New Era of Human Risk Governance (With a Practical Cyber Resilience Bill Playbook)

Introduction

The UK cyber security landscape has undergone a dramatic shift. In the past, cyber risk management focused primarily on firewalls, encryption, and other technical defences, with people often treated as a secondary concern. However, today the human element is at the heart of the risk equation, with the majority of successful attacks still involving human error or social engineering.

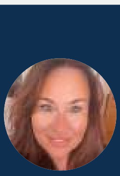
With cybercriminals increasingly targeting human vulnerabilities, UK organisations must develop strategic, data-driven human risk programmes that sit alongside technical controls. The UK Cyber Security & Resilience (Network and Information Systems) Bill (the "Cyber Security & Resilience Bill") is part of a wider move by government and regulators to strengthen governance, resilience and incident reporting across essential and important entities. While the Bill does not prescribe a specific "human risk" framework, it raises expectations on boards to evidence appropriate and proportionate measures across people, process and technology.

Boards and senior leadership are therefore expected to take clear ownership of cyber risk governance, including human-related risk, supported by guidance such as the NCSC Cyber Security Board Toolkit and the UK Cyber Governance Code of Practice. This whitepaper will explore the evolution of human risk management in UK organisations, the implications of the Cyber Security & Resilience Bill, and how organisations can develop board-ready human risk strategies that align with emerging UK regulatory expectations and demonstrate cyber resilience.

The Shift from Training to Governance

Cultural Evolution

In the past, human risk management in the UK was typically seen as a compliance task: annual security awareness training, basic phishing simulations, and simple tick-box exercises to satisfy policies or certification audits. The landscape has changed, and human risk management has evolved into a core strategic responsibility that goes beyond one-time events, particularly for organisations in scope of enhanced UK regulation and sectoral oversight. The Cyber Security & Resilience Bill, alongside the Cyber Governance Code of Practice, has helped drive a cultural shift towards board-level ownership of cyber security, with human factors recognised as a critical dimension of overall cyber risk.



**As Emma Hollinrake,
from Phishing Tackle explains:**

> *"What started as basic awareness training has now evolved into an entire industry focused on human risk management. It's no longer just about compliance; it's about actively protecting your organisation from cyber threats driven by human error."*

UK organisations can no longer simply rely on static training modules and sporadic phishing tests. Instead, they must adopt a proactive, data-driven approach to managing human risk that can stand up to board scrutiny and regulatory questions. The role of senior leadership is crucial, as government and regulators now expect boards to take ownership of cyber risk governance and to demonstrate how people-related risks are identified, managed, and monitored over time.

The Expanding Human Attack Surface

The New Threat Vectors

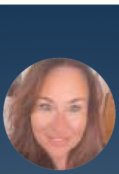
While email phishing remains one of the most common attack vectors, cyber threats are rapidly evolving. Attackers are increasingly targeting a wider set of digital platforms and communication channels used by UK workforces, including messaging apps, collaboration tools and QR codes, to exploit human vulnerabilities.

Key Threat Vectors:

1. **AI-assisted spear phishing:**
   Attackers use AI tools to craft highly targeted phishing messages personalised to the individual and organisation, making them harder to detect and filter.

2. **QR-based phishing ("quishing"):**
   Fraudulent QR codes are used to trick users into visiting malicious websites or downloading malware, for example via posters, emails or on-screen codes in shared spaces.

3. **Impersonation via collaboration tools:**
   Hackers impersonate colleagues or suppliers on platforms such as Microsoft Teams or Slack, sending fake messages with malicious links or requests for sensitive data, often bypassing traditional email-focused defences.



As Emma Hollinrake, from Phishing Tackle explains:

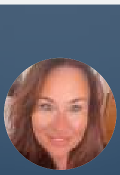
> *"The landscape has changed. Phishing is still a huge issue, but we are also seeing risks emerge through platforms like WhatsApp and Microsoft Teams. These new attack vectors require fresh training and testing strategies."*

To keep pace with this expanding human attack surface, UK organisations must move beyond traditional email-only phishing simulations and adopt multi-channel risk management strategies that reflect how staff actually communicate and work. This means designing training and testing that cover email, mobile, collaboration tools, QR codes and other channels used in day-to-day operations.

Why Traditional Awareness Models Fail

The Pitfalls of One-Time Training

UK organisations that continue to rely on one-off training sessions and annual phishing tests are leaving themselves exposed. Experience shows that infrequent, lengthy training does little to reduce human cyber risk in the long term, particularly in fast-changing threat environments.



As Emma Hollinrake highlights:

> *"What we've found is that regular testing and monthly bite-sized training modules are the most effective in reducing risk. Employees need consistent reminders to keep security top of mind."*

Limitations of Traditional Models:

Low engagement: Employees often complete long, infrequent training modules quickly, primarily to "get them done", with limited retention of key messages.

No reinforcement: Without consistent, bite-sized learning and regular testing, employees quickly forget critical security behaviours and reporting processes.

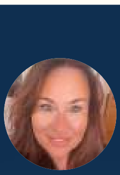
Completion ≠ risk reduction: Simply completing a training session does not mean an employee is less likely to fall for phishing or other social engineering attacks; what matters is behaviour during real or simulated incidents.

The future of human risk management in the UK lies in ongoing education, regular simulations, and continuous improvement, not one-off events. For boards and auditors, evidence of continuous, adaptive activity linked to measurable behavioural change will be much more compelling than simple "completion" statistics.

The Cyber Resilience Bill, What Changes

The Cyber Security & Resilience (Network and Information Systems) Bill is intended to strengthen the UK's cyber regulatory framework, particularly for operators of essential services, digital service providers and other critical organisations, by enhancing requirements around risk management, security and resilience, governance and incident reporting. It builds on, and in some areas goes beyond, the existing NIS regime and interacts with other UK initiatives such as the Cyber Governance Code of Practice.

While the Bill does not set out a dedicated "human risk" chapter, it expects in-scope organisations to adopt appropriate and proportionate technical and organisational measures, including staff training and awareness, to manage risks to the security and resilience of their network and information systems. The direction of travel is clear: boards will need to show they understand their exposure, have implemented controls across people, process and technology, and can evidence how those controls operate in practice.



Emma Hollinrake,
from Phishing Tackle stresses:

"Boards and shareholders are now demanding to know what organisations are doing to protect their data and people. It is no longer just a nice-to-have. If organisations fail to comply, the financial and reputational consequences are massive."

Key Changes Under the Cyber Resilience Bill:

Strategy: In-scope organisations must take a risk-based approach to cyber security and resilience, with governance arrangements that integrate cyber risk (including human factors) into overall organisational strategy and risk management.

Governance and oversight: Boards and directors are expected to take ownership of cyber security as a board-level issue, receiving regular reporting on cyber posture, including culture, training and human-behaviour risks.

Evidence and reporting: Organisations will need to demonstrate to regulators and, in some cases, insurers and other stakeholders that they have effective measures in place and that they learn lessons from incidents and near misses.

Controls and training: The Bill and associated guidance highlight the need for regular staff training and awareness as part of an appropriate control environment, especially in sectors where human error is a leading cause of incidents.

What Auditors Will Look For

The Cyber Security & Resilience Bill, together with emerging UK governance expectations, increases scrutiny of how organisations manage cyber risk in practice, not just on paper. While specific audit criteria will vary by sector and regulator, organisations should anticipate that auditors and regulators will expect clear, auditable evidence that human risk management is effective, proportionate and embedded.

Auditors and regulators are likely to focus on questions such as:

Frequency of testing: How often are employees tested on their ability to recognise and respond to threats, and does this extend beyond email to the main channels used by the organisation (for example, mobile, collaboration tools, QR codes)?

Multi-channel simulations: Are organisations conducting realistic simulations across email, mobile, collaboration platforms and other relevant channels, and adjusting scenarios based on emerging threats?

Evidence of remediation: How is follow-up training managed for employees who fail simulations or report incidents incorrectly, and is there a clear escalation and support process?

KPIs and risk scoring: How are organisations tracking and reporting improvements over time, for example through risk scores, behaviour-based metrics, reporting rates and time-to-report, rather than relying solely on raw “click rates” or training completion?

These types of measurable metrics and narratives are what UK businesses will increasingly need to show to boards, auditors and regulators to prove that their human risk management efforts are effective, appropriate for their risk profile, and aligned with the spirit of the Cyber Security & Resilience Bill.

Common Failure Points

Many UK organisations still rely on outdated methods that fail to address the evolving human risk landscape and do not align well with heightened expectations for governance and resilience. Common failures include:

One-off annual training with no ongoing reinforcement, leading to poor retention and limited impact on real-world behaviour.

Measuring click rates alone, rather than richer behavioural metrics such as reporting rates, time to report, or improvement over time in high-risk groups.

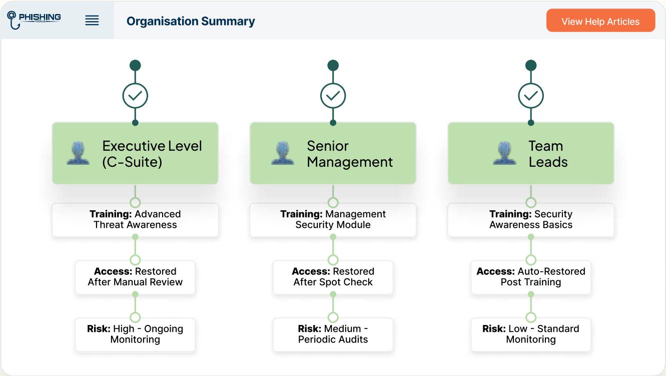
Manual reporting using outdated tools, which leads to inconsistent or incomplete data and makes it difficult to provide reliable board or regulator-ready reporting.

No clear ownership of human cyber risk at the board and executive level, with responsibilities fragmented across IT, HR, and compliance, and limited strategic oversight.

These gaps leave organisations exposed to significant risks at exactly the time when the UK regulatory bar is rising. The Cyber Security & Resilience Bill and related governance guidance make it harder to justify a purely "tick-box" approach to training and awareness; organisations will increasingly need to show that their activities are risk-based, measured and capable of continuous improvement.

Building a Board-Ready Human Risk Programme

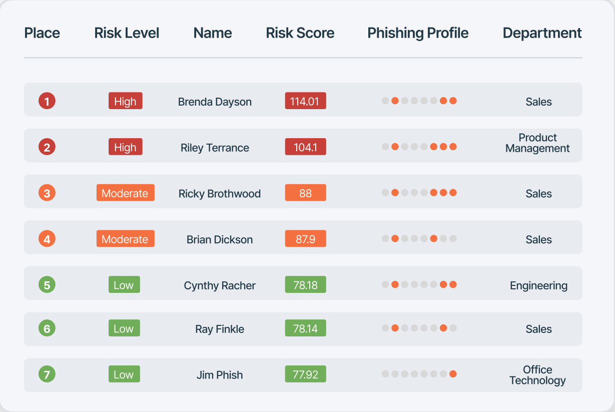
A comprehensive, UK-relevant human risk programme should help boards discharge their cyber governance responsibilities and build a defensible position under the Cyber Security & Resilience Bill and related expectations. Key components include:



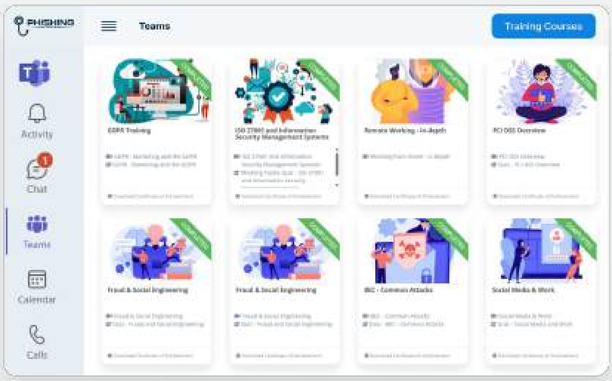
Executive Level (C-Suite)	Senior Management	Team Leads
Training: Advanced Threat Awareness	**Training:** Management Security Module	**Training:** Security Awareness Basics
Access: Restored After Manual Review	**Access:** Restored After Spot Check	**Access:** Auto-Restored Post Training
Risk: High - Ongoing Monitoring	**Risk:** Medium - Periodic Audits	**Risk:** Low - Standard Monitoring

Risk assessment framework: Identify human-related vulnerabilities based on role, region, department, and exposure to critical systems and data, aligned to your broader cyber and operational risk assessments.

Weighted scoring methodology: Use risk scoring to assess human risk at individual, team and organisational levels, with weighting that reflects the importance and privilege level of specific roles (for example, executives, finance, system administrators).



Place	Risk Level	Name	Risk Score	Phishing Profile	Department
1	High	Brenda Dayson	114.01	○●○○○○●●	Sales
2	High	Riley Terrance	104.1	○●○○○●●●	Product Management
3	Moderate	Ricky Brothwood	88	○●○○○●●●	Sales
4	Moderate	Brian Dickson	87.9	○●○○○●○○	Sales
5	Low	Cynthy Racher	78.18	○●○○○○●●	Engineering
6	Low	Ray Finkle	78.14	○●○○○○●○	Sales
7	Low	Jim Phish	77.92	○○○○○○○●	Office Technology


PHISHING
Teams
Training Courses
Activity
Chat
Teams
Calendar
Calls
GDPR Training
ISO 27001 and Information Security Management Systems
Remote Working - In-depth
PCI DSS Overview
Fraud & Social Engineering
Fraud & Social Engineering
BEC - Common Attacks
Social Media & Work

Continuous simulation engine: Run regular phishing and social engineering simulations across multiple channels (email, collaboration tools, QR codes, messaging) that reflect real-world attack patterns relevant to UK organisations.

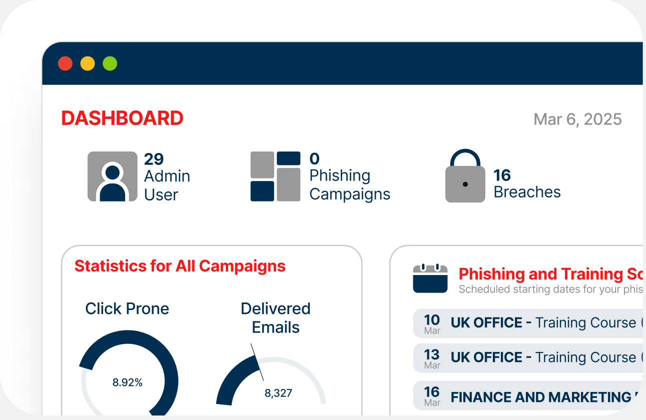
Micro-learning cadence: Provide ongoing, bite-sized training and nudges that are integrated into employees' normal workflow, with content tailored to observed risks and behaviours rather than generic annual courses.

Training and Resources

Security Induction - Training Course
Security Induction

Initial Training
Security Induction

August Admin
Bribery & C



DASHBOARD

Mar 6, 2025

29 Admin User

0 Phishing Campaigns

16 Breaches

Statistics for All Campaigns

Click Prone

8.92%

Delivered Emails

8,327

Phishing and Training Sc
Scheduled starting dates for your phis

10 Mar UK OFFICE - Training Course (

13 Mar UK OFFICE - Training Course (

16 Mar FINANCE AND MARKETING '

Automated board dashboards: Offer real-time or regular reporting on human risk metrics, trends and risk scores in a format that boards and executive committees can understand and act upon, aligned with broader cyber and operational risk dashboards.

Phishing Tackle's platform provides tools to help UK organisations manage human risk in this way, offering automated reporting, multi-channel testing and real-time insights that support compliance with the expectations underpinning the Cyber Security & Resilience Bill and the Cyber Governance Code of Practice. By integrating such a platform into their wider cyber governance structure, boards can obtain clearer assurance over how human-related risks are being monitored and reduced over time.

Conclusion, A Proactive Approach to Human Risk Governance

The Cyber Security & Resilience Bill signals a step change in how cyber security and resilience are governed in the UK, especially for organisations in critical and high-dependency sectors. It reinforces the principle that cyber is a board-level issue and that directors must be able to evidence appropriate, risk-based controls across people, process and technology. In this context, human risk can no longer be treated as a peripheral training task; it is a core pillar of cyber resilience.

A robust human risk strategy for UK organisations requires clear ownership, role-specific training, continuous monitoring and evidence that behaviour is improving over time. Platforms such as Phishing Tackle can play a key role in delivering multi-channel simulations, micro-learning and board-ready analytics that help organisations align with UK regulatory expectations and strengthen their overall security posture.

UK organisations that want to stay ahead of the Cyber Security & Resilience Bill, the Cyber Governance Code of Practice and evolving stakeholder expectations should consider a Human Risk Governance Review. This can help boards understand their current human risk exposure, benchmark against best practice, and build a roadmap for a truly data-driven, board-ready human risk programme.

Book a demo

PHISHING TACKLE