PhishRod.
Addressing Human Risk

Cybersecurity Behaviour Maturity Model

From Reactive to Proactive

Executive Summary

Human Risk and Behaviour Maturity in cybersecurity is the process of systematically assessing and improving how well an organisation manages cybersecurity risks stemming from human behaviour, such as errors, non-compliance, social engineering susceptibility, and unsafe digital habits.

Organisations use multiple controls (set of technologies and processes) to mitigate human risk by creating security awareness to build a cyber secure culture. It requires conducting a set of activities such as exposure assessments, phishing simulations, security awareness campaigns & policy enforcements to ensure that end users play their role in protecting the digital boundaries of the organisation.

PhishRod has developed a Cybersecurity Behaviour Maturity Model that outlines and categorises the steps that should be taken by an organisation to build a programme that revolves around assessing end user behaviour, creating cybersecurity awareness and empowering end users to build a cyber secure culture.

Understanding Human Risk Management

Human Risk Management (HRM) is a holistic approach to cybersecurity that revolves around understanding, measuring, and mitigating the risks associated with human behaviour. Despite technological advancements, human error remains the leading cause of cybersecurity breaches, making this a critical area of focus.

Mitigating Human Risk

Mitigating human risk requires carefully assessing human security behaviours and profiling end users by quantifying human risk. It focuses on building an effective behaviour maturity programme that focuses on:

- Empowering end users to protect themselves and their organisation
- Creating a cyber secure culture
- Monitoring end user behaviour
- Measuring and improving continuously

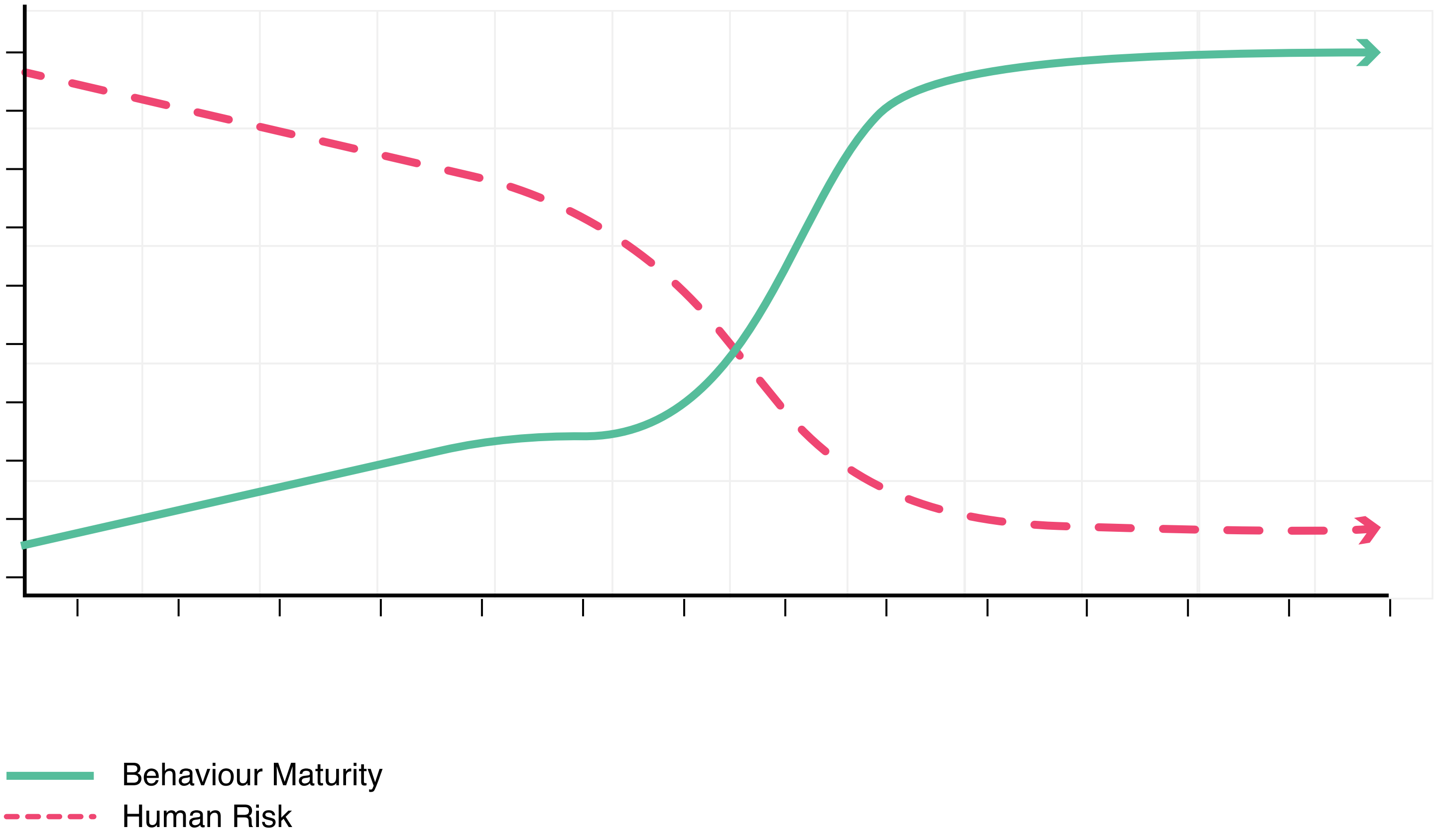
Modern Day Threat Landscape and Human Risk

As cyber defences become stronger technologically, attackers increasingly focus on manipulating people, making human risk one of the most critical aspects of cybersecurity today. The rise in AI-Powered Phishing Attacks, Deepfakes and Social Engineering continues to prove that humans are the number one attack vector for cyber adversaries.

A cybersecurity incident took place at ARUP, where an adversary used a deepfake zoom call, impersonated the CFO and lured the finance controller to transfer USD 25M, is a reminder that humans are vulnerable. Such was the impact of this incident that the cybersecurity industry coined the term “Digitally Cloned CFO” for such types of attacks.

Correlating Human Risk and Cybersecurity Behaviour Maturity

The more an organisation invests in Cybersecurity Behaviour Maturity, the lesser the human risk. As the organisational behaviour maturity increases, the end users become more aware and contribute proactively to mitigate threats that are targeted towards them. This initiates a process of self-accountability as they understand the impacts of clicking an unwanted link or sharing confidential data. Cybersecurity Behaviour Maturity ensures that end users are aware of the cyber threats and comply to the cybersecurity policies set out by the organisation resulting in higher compliance and reduced risks. As Cybersecurity Behaviour Maturity evolves gradually, the trust in the internal systems and people increases.

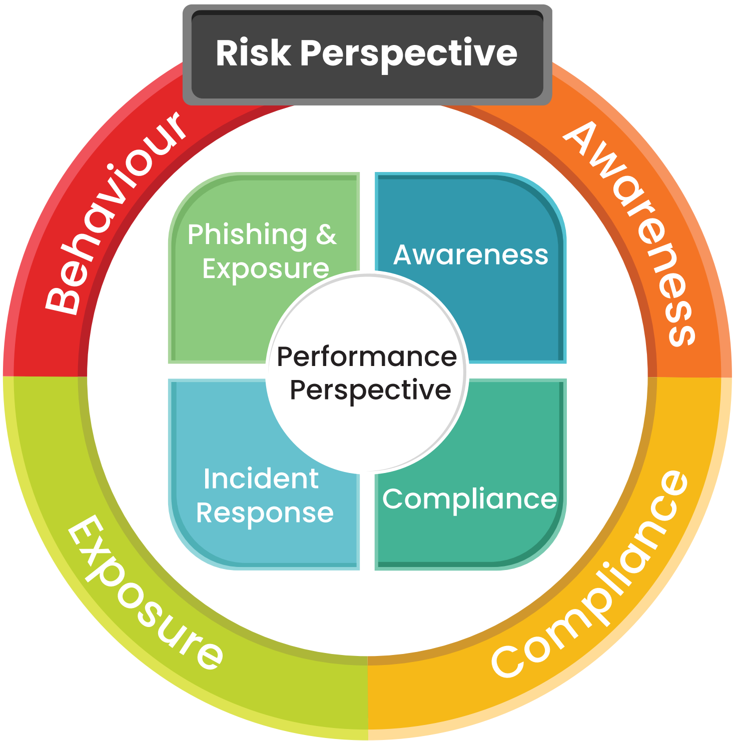


PhishRod and Human Risk Management

PhishRod is a global leader in human risk management that offers a holistic approach for minimising human risk, from assessment, awareness to incident response and policy compliance. Our integrated, data-driven approach helps turn vulnerable end users into active defence agents.

At PhishRod, Human Risk Management is at the core of our mission to transform end users from the weakest link into the strongest line of defence. Our strategy goes beyond conventional security awareness by providing a targeted, data driven approach. The goal is simple: empower organisations to reduce human-related cyber risks and help them achieve higher Cybersecurity Behaviour Maturity.

We achieve this by identifying high-risk users through continuous behavioural analysis and phishing simulations. Our platform enables automated security awareness programmes tailored to individual risk profiles, ensuring that training is relevant, timely, and effective. Through integrated Policy Compliance Management, we drive adherence to organisational policies, while our Incident Reporting and Response modules enable users to act as real-time threat sensors within the organisation.



Our analytics driven approach ensures that Human Risk Indicators (HRIs) are measured and monitored throughout the Cybersecurity Behaviour Maturity lifecycle. The KPIs across Security Awareness, Security Behaviour, Phishing Readiness, Policy Compliance, Incident Response and existing exposure to breaches are measured from both performance and risk perspective.

Cybersecurity Behaviour Maturity Model

PhishRod has developed the Cybersecurity Behaviour Maturity Model that guides organisations to build a cyber secure culture. The model is built on the experience and expertise that we acquired while working with diverse customers globally. The model benchmarks organisations across various levels of maturity based on the series of activities they are conducting to address human risk.

It's designed to guide organisations in understanding where they stand and what steps are necessary to improve the security mindset and actions of their workforce.

Level	Description	Key Characteristics
Reactive	End users not fully aware of cybersecurity threats. Incidents are frequent	• Compliance driven awareness only • No focus on cyber hygiene • High risk of incidents
Defined	End users follow basic cybersecurity hygiene, security awareness structure in place	• Users know basic threats (phishing, social engineering) • Behaviours inconsistent
Integrated	Users take part in security awareness and policy compliance but may not fully understand why.	• Training is regular • Policies are followed • KPIs related to security awareness and policy compliance exist
Adaptive	Cybersecurity is a shared responsibility.	• Security embedded in daily work • Accountability based on KPIs • Reporting of incidents increases • Security Champions lead the initiative
Proactive	Human Risk is managed proactively and remains core of the cybersecurity strategy.	• Monitoring of Security Behaviours • User Profiling based on Quantitative Risk KPIs • Threshold for human risk index defined at user and organisational level. • Behaviour insights drive the policy • Continuous feedback and improvement

Level 1: Reactive

At this level, behaviour maturity efforts are triggered by incidents or compliance requirements rather than being part of a strategic plan. Organisations respond to human risk after it occurs, not in anticipation of them.

Organisations at this level, generally opt to conduct security awareness trainings either manually or through an automated tool. There is no role-based training. The KPIs are only limited to the status of completion of the assigned security awareness material. The medium for awareness is limited to classroom led sessions or computer-based training modules only. There is no quarterly or annual security awareness plan with minimal or no focus on cyber hygiene.

Since the focus is on meeting internal audit or regulatory requirements, it fails to meet the objectives thereby giving a false sense of security.

Level 2: Defined

Organisations at this level understand the value of the security behaviour management however the implementation of an effective programme is missing. The focus remains on creating awareness, a formal security awareness programme is in place. Security awareness is conducted using multiple modes such as Computer-Based Training modules, newsletters, posters and infographics. To determine the end user behaviour, Phishing Simulation exercises are conducted but users are not tested against advanced phishing techniques. Phishing Index for organisations at level 2 is generally higher. End users are not exposed to Smishing or Vishing tests hence the behaviour of end users is tested only to a limited scale. Empowerment tools such as the ability of end users to report suspicious or simulated phishing emails is not in place resulting in inconsistent security behaviours.

Level 3: Integrated

At this level, organisations follow a much more structured approach to security behaviour management. Cyber Skills Surveys are conducted, and security awareness programmes are designed based on their results. The content is carefully selected; customised content is often preferred that focuses on highlighting the organisation's cybersecurity policies. Cybersecurity content is assigned based on the roles and the security behaviour maturity programme has the backing of the senior management. Security Awareness and Policy compliance is integrated, and user profiles include KPIs for both. It is mandatory for end users to go through cybersecurity policies. The vendors are also provided awareness on the cybersecurity policies of the organisations ensuring minimal risk related to supply chain attacks.

Phishing readiness is conducted at an advanced level with end users empowered to report suspicious emails thereby encouraging positive security habits. Exposure assessments are conducted at regular intervals to determine any possible exposure of personal and corporate information on the dark web.

At this stage the efforts of an organisation related to transforming end user behaviour start to show results with Security Awareness and Policy Compliance Index being higher and Phishing Index being lower. Organisations at this stage often expose end users to advanced behaviour tests such as Vishing, Smishing and USB drop tests.

Level 4: Adaptive

It is at this level that organisations start to view the results of Cybersecurity Behaviour Maturity from the lens of human risk. The objective of security awareness, policy compliance and phishing readiness is geared towards security behaviour management and KPIs are collected from both performance and risk perspective. It is at this stage that organisations have well defined policies for human risk and behaviour management. Organisations gather data related to behaviour management, review it on a monthly or quarterly basis. Security Awareness Champions or change agents for behaviour are assigned to work with every department to convey the message that "cybersecurity is a shared responsibility". Organisations also conduct cybersecurity awareness events and engage end users in more unconventional ways of creating security awareness. Based on the ongoing security awareness and policy enforcement, less cybersecurity incidents related to human behaviour are reported and end users are accountable for their actions. End users with risky behaviours are reported to the management/HR and a structured incentive/reprimand programme is in place.

End users fully understand that their risk profiles are being built and analysed. There is an open culture in the organisation related to cybersecurity, cybersecurity advisories are shared, and results of phishing readiness are shared within the organisation. KPIs are in place at the organisation, department and user level and minimum acceptable level of human risk is documented.

Level 5: Proactive

It is the highest level of Cybersecurity Behaviour Maturity where human risk is proactively managed by transforming end user behaviour. Organisations at this stage have a cyber secure culture governed by tools, processes and policies. Monitoring security behaviour is a key to reach this level where organisations go beyond conventional security awareness and compliance initiatives.

Organisations use data from 3rd party tools such as SIEM or DLP to monitor the end user behaviour and determine end users with risky behaviours. Vulnerable end user behaviour such as plugging a USB storage device, suspicious login attempts, execution of exe files, sending confidential data, downloading mass files is monitored for every end user and violation alerts are sent to end users in real time.The moment an end user makes a violation, immediately a security awareness training or a corporate security policy related to the type of the violation is sent to the end user. Each violation against security behaviour monitoring has a weightage and contributes to the Human Risk Index.

Security Behaviour Monitoring

- USB Storage Detected
- App Execution from
- Downloads/Documents
- Multiple Login Failure
- Suspicion Login Activity
- Msi and Exe Execution
- Unusual Geolocation
- Unusual Traffic Surge
- Suspicious SharePoint activity
- Clipboard Monitoring
- Screen Capture Tool Detection
- Outbound Network Connection Logging
- Executable Drop to Temp/AppData
- Persistence Detection (Registry/Tasks)
- Office App Spawning Shells
- Executable Masquerading as .txt/.jpg

Quantitative analysis remains the core at this level. Besides performance data on security awareness, policy compliance and phishing readiness, the users are shown the policy violations that they have committed over a period of time. A structured human risk management approach is in place with a minimum acceptable risk threshold across the organisation and all efforts are made to keep the human risk under that threshold.

Security Awareness is part of onboarding, performance reviews, and team goals. Security training is sought out, not mandated and alternative mediums such as chatbots and other mediums are available for end users to increase their knowledge about cyber threats voluntarily.

Conclusion

As the digital threat landscape continues to evolve, the ability of an organisation to manage and reduce human risk has become a critical determinant of its cybersecurity resilience. The Cybersecurity Behaviour Maturity Model provides a structured pathway for organisations to evaluate and enhance their behavioural defences, moving from reactive awareness to a proactive, data-driven culture of security. By embedding security behaviours into daily workflows, aligning them with measurable KPIs, and continuously refining their approach, organisations can significantly reduce human-induced vulnerabilities.

About PhishRod

PhishRod is a global leader in Human Risk Management, empowering organisations to mitigate cyber threats linked to vulnerable end-user behaviour. By leveraging advanced analytics, behaviour monitoring, personalised training, policy compliance, and continuous profiling through phishing simulations, PhishRod delivers a comprehensive, data-driven approach. Backed by global expertise, we help enterprises shift from Reactive to Proactive Maturity Level, minimising human risk and strengthening overall cyber resilience. For more information, please visit **www.phishrod.co**

PhishRod®
Addressing Human Risk

Corporate Head Office:
176 Outwest, Irvine, CA 92618

PhishRodAddressingHumanRisk

company/phishrod

phishrod_co

Contact Us: info@phishrod.co