

HUMAN RISK MANAGEMENT

THE NEW FRONTIER OF CYBERSECURITY

Employees are the cornerstone of every organization, but they also represent a significant cybersecurity risk.

While Security Awareness Training (SAT) is important, it often falls short in addressing the complex & evolving nature of cyber threats. It focuses too much on compliance with one-size-fits-all training & has limited impact on behavior change.

HRM puts human behavior at the forefront of cybersecurity by focusing on:



Driving behavioral change

Fostering a security-conscious culture



Measuring impact on reducing security incidents

HRM Approach

Monitor if the targetted group's behaviour has changed



The Changes Brought By HRM

SAT		HRM
Primarily focuses on educating employees about security threats & best practices	FOCUS	Goes beyond education to proactively identify, assess & mitigate human-related security risks
Often generic, one-size-fits-all content	APPROACH	Tailored to individual roles, responsibilities & behaviors
Raise awareness of security risks, promote compliance with policies	GOALS	Reduce human-related security incidents, foster a security-conscious culture
Online modules, workshops, phishing simulations	METHODS	Risk assessments, behavioral analysis, threat intelligence, targeted security awareness training
May improve employee knowledge but doesn't always lead to significant behavior change	IMPACT	Aims to drive measurable changes in behavior & reduce human-related security incidents