SECURITY AWARENESS TRAINING IS BROKEN.

WHY HUMAN RISK MANAGEMENT (HRM) IS THE NEW FIX FOR CREATING A SECURITY-SAVVY WORKFORCE.

usecure

www.usecure.io

Intro

Don’t be fooled...

Businesses are investing more than ever into strengthening their human resilience against evolving cyber threats, but a big problem still plagues SMBs and enterprises in every sector — user-related data breaches.

Even with more businesses rolling out security awareness training measures, 85% of data breaches still involve the human element (*Verizon, DBIR 2021*).

But why is this?

In this guide, we look at why traditional security awareness training often isn't enough to transform user behaviour, and how businesses can truly create a security-savvy workforce through the new class of user-focused security...

Human Risk Management (HRM).

Contents

Why do modern businesses need to manage human cyber risk? 01-02

Why isn't traditional security awareness training enough? 03-04

How does Human Risk Management (HRM) provide the fix? 05

How does HRM work? 06

How does HRM create a security-savvy workforce? 07

How does usecure simplify HRM? 08

Start calculating human risk today 09

Why do modern businesses need to manage human cyber risk?

Employees play a huge role in keeping systems and sensitive data safe which, in the wrong hands, can cause hefty financial, operational and reputational damage.

Bad news is, employees make mistakes, with Verizon stating that 85% of data breaches still involve the human element.

Here are **three reasons** why managing human cyber risk is so vital for today's businesses...

#1 Human error is a big problem

Whether it's typos or forgetting passwords, mistakes at work happen every day.

Unfortunately, supposedly small mistakes like downloading an attachment from an unknown sender or misdirecting an email on a burnt-out Friday afternoon can cause more than just a red face - with IBM reporting that **human error is a major contributing cause in 95% of all breaches**.

Whether it's down to lack of awareness or just a momentary lapse of judgement, businesses need to train their users to reduce costly mistakes.

#2 Employees break the rules

Sometimes, rule-breaking can be done with malicious intent, like a disgruntled ex-employee stealing mountains of data and selling this on to scammers or whoever else is willing to buy.

According to IBM's Insider Theft Report, insider threats (including employee data theft) have **cost companies** $11.45M and incidents have tripled since 2016.

Other times, employees might just be trying to cut corners to make their lives a little easier, like reusing the same password for multiple accounts.

#3 Your human firewall can be exploited

Many of today's cyber attacks are geared towards manipulating employees, often with criminals using phishing attacks to impersonate customers, colleagues, contractors and suppliers.

The tricky part is, it only takes one mistake from an employee to cause a ripple of repercussions - with phishing scams costing US businesses adjusted losses of over 54 million dollars *(FBI's IC3 Report)*.

Attacks like Business Email Compromise (BEC) and targeted phishing will only keep increasing, with Google recently reporting that there are now 75 times as many phishing sites as there are malware sites on the internet.

Why does traditional security awareness training often fall flat?

It's easy to think that rolling out security awareness courses and sending a few email bulletins from time to time is enough to make employees behave more securely.

But computer-based security awareness training and send-to-all cyber tips often aren't enough to truly boost user resilience and drive secure human behaviour.

Here's why traditional security awareness training measures often fall flat:

Too focused on ticking the boxes

Traditional user training has been heavily geared towards finding the training content, delivering the training, and then (maybe) testing what the users have learned. This simplistic approach pays more focus on delivering training, rather than delivering a solution for tackling human risk.

Training is too irregular

A lot can be asked of employees when delivering a one-hour, yearly workshop. Staff are expected to understand the information, retain it and then use it. Problem is, we all forget things and new attack techniques are popping up all of the time.

Training is too generic

Some employees are highly vulnerable to phishing but cautious with password hygiene. Some employees have weak passwords that they re-use, but rarely forget to log out of their devices. Point is, every employee has a unique set of risk areas. Send-to-all training courses don't address each users' knowledge gaps.

The impact often isn't measured

This is a big one. Like anything in life, if we don't measure performance, how do we know things are improving? Once training has been delivered, it's important to measure what the employees have actually retained.

Cyber reflexes often aren't tested

Just like athletes, people can look great in training, but how does this translate into a real-world event? Deploying practical tests, like phishing simulations, is an effective way of measuring the impact of training and understanding ongoing risks to real-world attacks.

The source of the problems isn't tackled

61% of breaches involve stolen user credentials - like usernames and passwords - many of which are exposed on the dark web. These credentials are then used to fuel social engineering and spear-phishing attacks against users. Security awareness programs often don't address this issue, even though it is a hugely popular asset that provides ammunition for many attacks.

Policies get overlooked

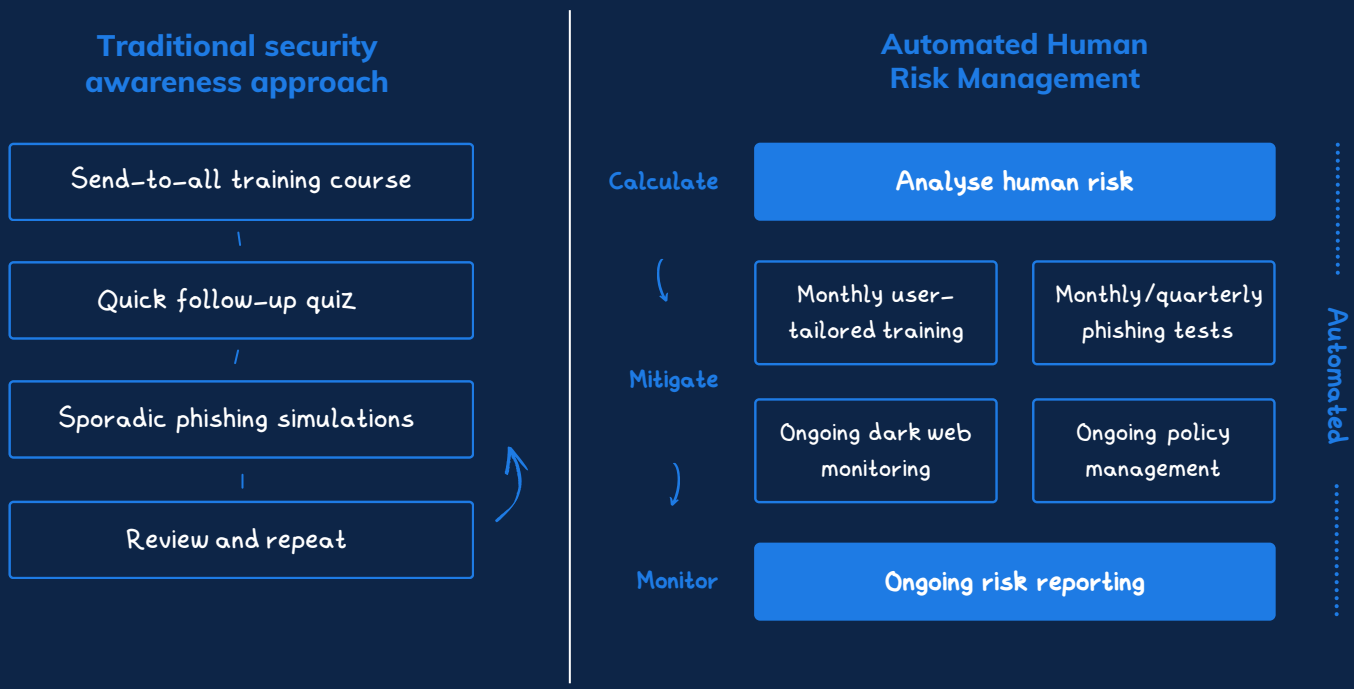
Sometimes, employees are oblivious to their responsibilities as a key security cog in the business. Often, this is due to a lack of clear communication when it comes to security policies and processes. Employees need to understand what security behaviour is expected of them and why this is so important.

How does Human Risk Management (HRM) provide the fix?

> Human Risk Management is the new class of user-focused security that empowers businesses to understand, reduce and monitor their employee cyber risk — without having to sacrifice productivity for protection.

Whereas businesses typically deploy security awareness training programs to reduce employee risk, HRM offers a full-circle solution for transforming humans into a business' strongest defence against evolving threats.

Traditional security awareness training VS Human Risk Management (HRM)



How does HRM work?

Traditional training is built on the idea that humans are the "weakest link in the cyber security chain". Human Risk Management is built on the belief that humans are an organisation's strongest line of defence against evolving cyber threats - your business just needs the right tools to get them there.

The key ingredients for making HRM work

To make sure that employee cyber risk is continuously being tackled, usecure's HRM platform automates the following features:

Regular cyber awareness training → Personalised video and interactive training programs are created for every user, with bite-sized courses and follow-up quizzes being automatically sent each month.

Periodic employee phishing simulations → Regular phishing simulations are automatically deployed that assess user vulnerability to a range of attack techniques. Custom phishing campaigns can be created in minutes.

Clear policy approval process → Policies are centralised in one easily accessible place and staff are automatically notified of any updated policies that they need to sign, with staff approval signatures being tracked.

Ongoing dark web breach monitoring → Continuous dark web monitoring detects when sensitive company data (e.g. usernames and passwords) has appeared in a data breach, which could be used for targeted attacks.

Human risk monitoring → Human risk is continuously tracked, with insight-rich reporting and human risk scoring. Dig deep into training performance and phishing trends straight from your dashboard.

How HRM creates a security-savvy workforce

Regular bite-sized training

Micro training courses are automatically delivered to each user every month to keep training frequent without hindering productivity.

Personalised training for every user

To start with, each users' core security knowledge gaps are assessed during a quick 10-min Gap Analysis Quiz and then, from their answers, an ongoing and personalised training program is deployed with prioritised courses.

Easily understand the ongoing risk

Before launching your HRM program, usecure will calculate your organisation's Human Risk Score to give a benchmark of your employee security posture. Then, multiple metrics (incl. phishing, training and dark web results) are fused together to give an overview of how user risk is changing over time.

Users are tested against real-world attacks

Regular phishing simulations are automated to help monitor each users' vulnerability to a range of evolving attack techniques.

Keep users well-versed on their responsibilities

Policy management and communications are made simple with an easy-to-navigate document library and automated eSign approval tracking that eliminates the time and hassle of chasing staff signatures.

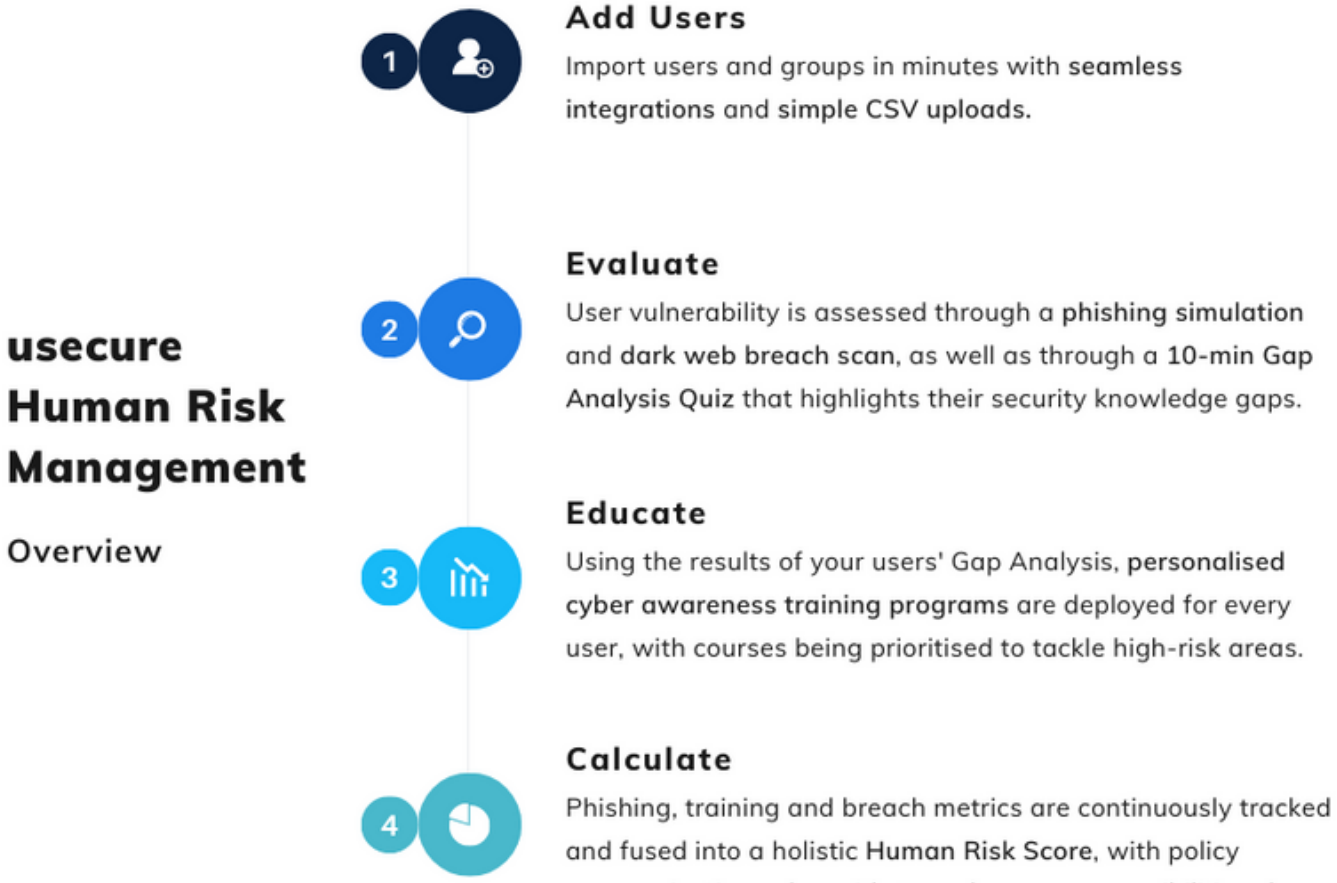
Detect early stage user threats

Ongoing dark web monitoring detects when employee credentials are compromised and up for grabs on the dark web, with additional insight into what service led to the breach and what type of data is exposed.

How does usecure simplify HRM?

It can seem a bit daunting when thinking about launching, managing and measuring a risk management solution.

That's why usecure's Human Risk Management platform uses an automated and simplified approach that makes deployment and admin super easy. Here's how it works:



See usecure in action

Watch bite-sized demos to learn how usecure tackles human cyber risk.

Watch a demo »

Get Started Today

Start calculating human cyber risk today

Watch bite-sized demos to learn how usecure can transform your organisation's human cyber risk.

Get Started »

www.usecure.io