HUMAN RISK MANAGEMENT (HRM) CASE STUDY

First-hand look at how HRM transformed this business's employee security behaviour.

CUSTOMER OBJECTIVES

- Identify which employees are at high risk of being compromised in a phishing attack
- Obtain an ongoing view of which employees are vulnerable to phishing attacks
- Deliver regular security awareness training that will help drive user resilience to phishing attacks, as well to improve general security behaviour
- Demonstrate compliance with ISO 27001 Clause 7.2.2

APPROACH

Security Awareness Training

- Analyse each users' current security strengths and weaknesses using a Gap Analysis Quiz.
- Using the results of the quiz, each employee will receive a new security awareness course every four weeks, with courses being prioritised to address their weakest areas first.
- Custom compliance courses will also be delivered periodically.

Simulated Phishing Exercises

- At least one phishing simulation will be launched every six months, in order to test the impact of the training and to identify any high-risk users.
- Instant follow-up training will be deployed to any employees who compromise their credentials during a phishing simulation, in order to reduce risk as soon as possible.

Dark Web Monitoring

- Ongoing dark web monitoring will take place in order to identify and avoid early-stage attacks that leverage stolen employee credentials, like compromised usernames and passwords.

CUSTOMER PROFILE

Industry

- Construction

User Count

- 250 Employees

Using Service Since

- August 2020

CHALLENGES/ KEY DRIVERS

- Member of staff was compromised in a 'Gift Card' phishing attack
- Current security awareness training materials are unengaging and ineffective
- Current security awareness training approach is too time-consuming

THE IMPACT - RISK SCORE

In order to measure the impact of the customer's Human Risk Management program, key risk metrics were taken both at the very start of the program and after seven months of activity.

Below, you'll see the '**company**' risk score (all risk metrics fused together), a '**training**' risk score, (a combination of course grades and course completion percentages), a '**phishing**' risk score (the collated opened, clicked and compromised rates during phishing simulations) and a '**dark web**' risk score (based on how much of your business's sensitive data is exposed on the dark web).

RISK SCORE

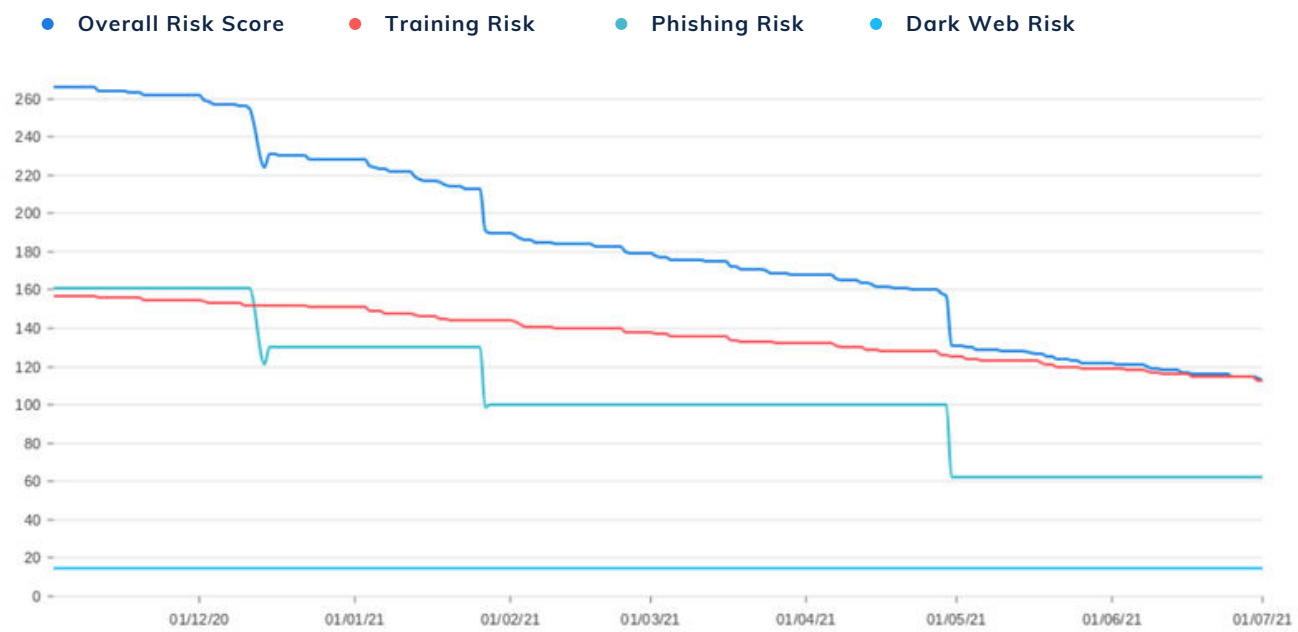
Having conducted seven months of security awareness training, periodic simulated phishing exercises and dark web breach scanning, the customer's overall human risk score was reduced by 152 points - moving them from '**Medium**' risk to '**Low**' risk.

The phishing risk within the business drastically decreased by 100 points, meaning that the employees were considerably better at spotting, avoiding and reporting suspected attacks.

INITIAL RISK SCORE		RISK SCORE AFTER 7 MONTHS
270/900	»	**118**/900
Medium		Low

KEY METRICS

- COMPANY RISK | -152
- TRAINING RISK | -40
- PHISHING RISK | -100
- DARK WEB RISK | NO CHANGE



THE IMPACT - TRAINING & PHISHING RESULTS

In order to reduce human cyber risk, it was important to ensure that employees were completing their security awareness courses as soon as possible and reaching the minimum pass score of 80% in their follow-up questionnaires.

To ensure this happened, the completion rate and course grades were tracked for every employee, with automatic course reminder emails being sent out to any staff members who hadn't completed their course within a few working days.

The ongoing phishing simulation results were also tracked to ensure that the security awareness training courses were having the desired impact.

TRAINING ADOPTION

Avg. time to complete a course after enrolment	Courses Started	Course Completed	Average Course Grade
3 Days	97%	97%	92%

PHISHING SIMULATION PERFORMANCE

	Sent	Opened	Visited	Compromised
1st Simulation	146	74	40	9
2nd Simulation	172	34 -74%	4 -163%	2 -127%

Out of the 250 staff, 97% per cent started and completed their courses, taking on average just three days to finish their course after enrolment, whilst scoring, on average, 92%.

As seen in the Phishing Simulation Performance table, employees were much less likely to open, click or become compromised by a phishing simulation.