FOX Technologies

CASE STUDY

Human Risk Management

Learn how a leading engineering company transformed its security culture in less than six months.

439 ↘

The overall human risk score dropped from 575 to 136, down by 439 risk points.

96%

of employees had completed the 12 beginners courses within six months.

303 ↘

The biggest reduction in risk came in phishing, down by 303 risk points.

CUSTOMER PROFILE

Leading engineering company trusted for advanced medical and surgical solutions in Singapore.

INDUSTRY

Engineering

EMPLOYEE COUNT

86

HEADQUARTERS

Singapore

USED SERVICE SINCE

January 2022

DATE OF CASE STUDY

May 2022

CHALLENGES

1. **STAFF DATA PROTECTION BEHAVIOUR**

   As a leading engineering company with a trusted reputation, this customer needed to ensure its staff were well-versed in data protection.

2. **INCREASE IN PHISHING THREATS**

   With phishing attacks increasing in frequency and sophistication, employees needed to be assessed and trained in spotting these attacks.

3. **REDUCING HUMAN ERROR**

   With human error being the number one cause of data breaches, training employees on general cybersecurity best practice is vital.

OBJECTIVE | THE ROAD TO REDUCING RISK

Given the challenges this customer was experiencing, they set out to assess their existing employee security posture in order to identify their biggest human risk areas, and then strengthen these vulnerable areas through regular user training, phishing simulations and dark web monitoring.

1 GAP ANALYSIS

An initial gap analysis questionnaire will be sent to each employee to assess their security knowledge gaps, highlighting in which areas they most need training.

2 END-USER TRAINING

Using the gap analysis results, employees will be enrolled onto a personal training program that sends one course per week, with a **minimum pass score set at 85%**.

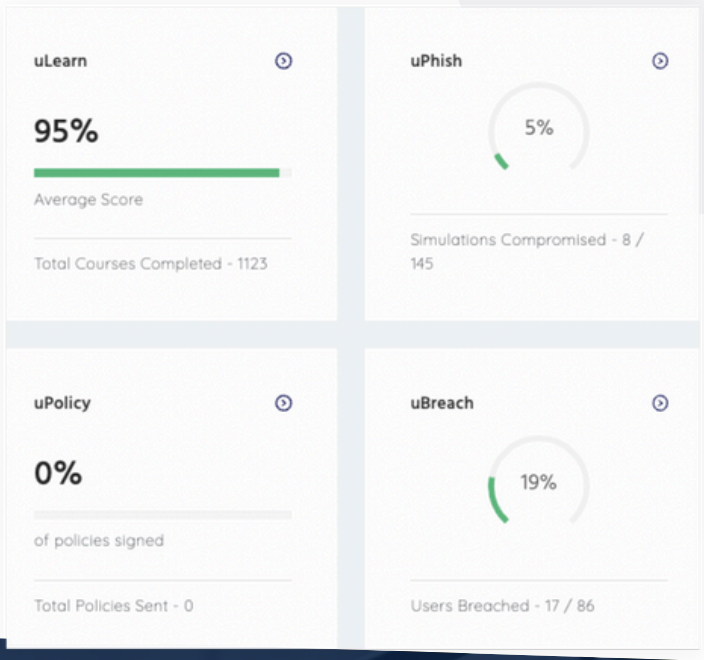
4 BREACH MONITORING

Ongoing dark web monitoring will be run to help identify and prevent early-stage cyber attacks that could leverage stolen employee credentials for phishing.

3 PHISHING SIMULATIONS

Periodic phishing simulations will be deployed in order to track which employees are vulnerable to phishing, and to help assess the training impact.

RESULTS | JAN - MAY PERFORMANCE



After almost six months, these were the end results in each area:

GAP ANALYSIS

- The gap analysis questionnaire was completed by **100%** of staff

END-USER TRAINING [ULEARN]

- Courses completed: **1,123**
- Average course score: **95%**

PHISHING SIMULATIONS [UPHISH]

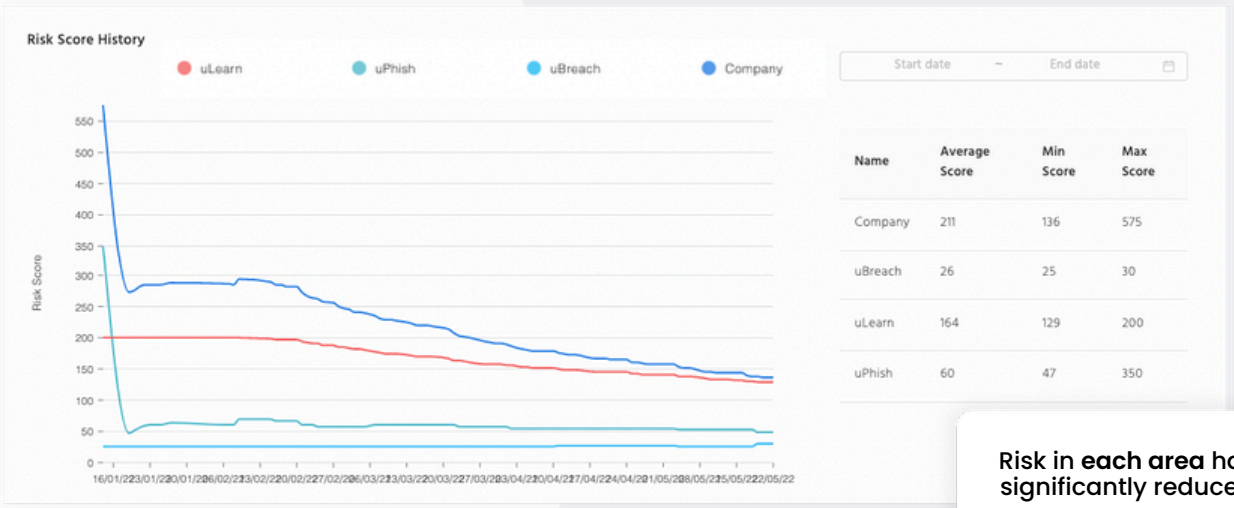
- Simulation campaigns sent: **145**
- Simulations campaigns that led to an employee being compromised: **8** *(5% of simulations)*

BREACH MONITORING [UBREACH]

- No. of employees with credentials (e.g. usernames and passwords) found in a data breach: **17** *(19% of staff)*

HUMAN RISK SCORING | MAKING SENSE OF THE DATA

To truly understand how employee cyber risk is changing in the business, our service fuses multiple data sets together into one holistic human risk score, helping you to contextualise the training, phishing and dark web breach performance in a digestible and actionable way. Below shows the engineering company's overall risk score change over time, as well as in each core area.



Risk in each area has significantly reduced

As you can see in the 'Risk Score History' graph above (also listed below for easy viewing), human risk was reduced in each core area and the company as a whole. Overall, human risk was reduced by 439 points, ending with a **'Good' risk score of 136/900** (900 being the worst score possible).

The **biggest improvement came in the reduction in phishing risk**, with the overall risk score ending in 47/550, reducing by 303 points as less employees became compromised in simulations.

COMPANY RISK SCORE

- January 2022 - **575**
- May 2022 - **136 (-439)**

UBREACH

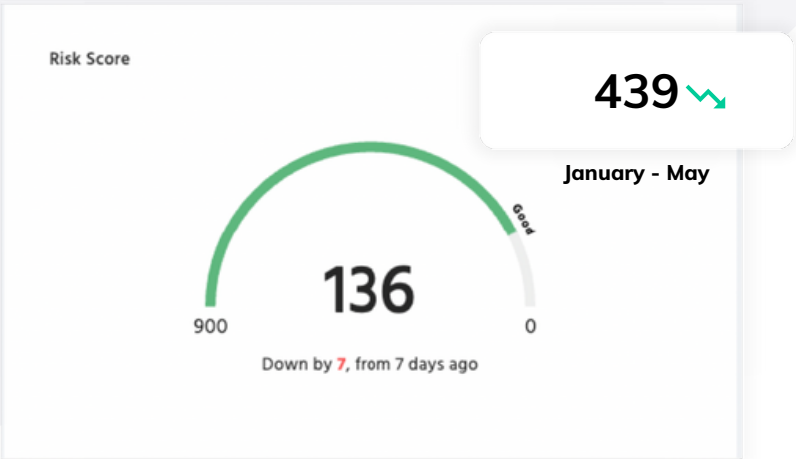
- January 2022 - **30**
- May 2022 - **25 (-5)**

ULEARN

- January 2022 - **200**
- May 2022 - **129 (-71)**

UPHISH

- January 2022 - **350**
- May 2022 - **47 (-303)**



Company-wide risk is scored out of 900.

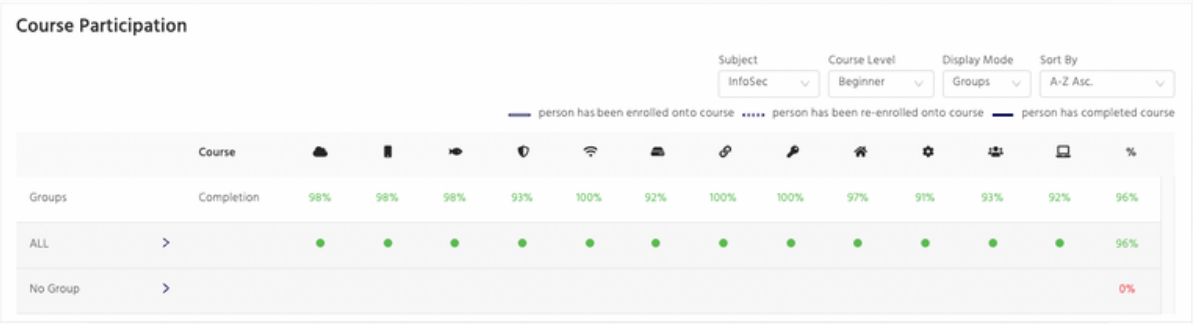
Individual areas (i.e. uPhish, uLearn, etc) are scored out of 550.

The higher the score, the higher the risk.

END-USER TRAINING | PARTICIPATION AND PROGRESS

It may sound obvious, but one key factor for improving employee security behaviour is by making sure that everyone is consistently completing their training courses. That's why we make our training courses short, engaging and self-paced, helping to keep course participation and impact high.

As you'll see the engineering company's report below, **we track a number of key metrics that measure how end-users are progressing in their training journeys**.



The table above outlines how many end-users have completed each of the 12 'Beginner' stage courses. **Overall, 96% of end-users have already completed all beginner stage courses**.

Our service also tracks the completion rate for the 'Intermediate' and 'Advanced' courses. Here is how the engineering company's employees performed between January to May 2022:

January ..... May

100%	96%	66%	48%
of end-users completed the gap analysis	of end-users completed the beginner courses	of end-users completed the intermediate courses	of end-users completed the advanced courses