

# Human Vulnerability Assessment: Explained



# Human Vulnerability Assessment (HVA)

## **What is it?**

A series of questions relating back to all of our cybersecurity modules.

## **Why is it needed?**

Rather than providing blanket training to all staff, the HVA aims to identify weak areas in organisational cybersecurity knowledge and prioritise training based on the results.

## **What does it do?**

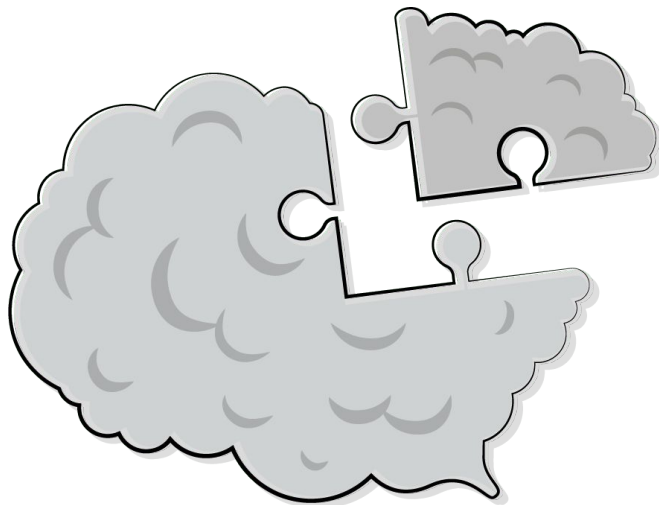
It aims to measure 9 key behavioural factors which will be explained in this booklet.

## **What are the benefits?**

These factors allow us to assess key organisational risks. These are compared to employees' actual behaviour through the use of a phishing simulation and course progress throughout the year.

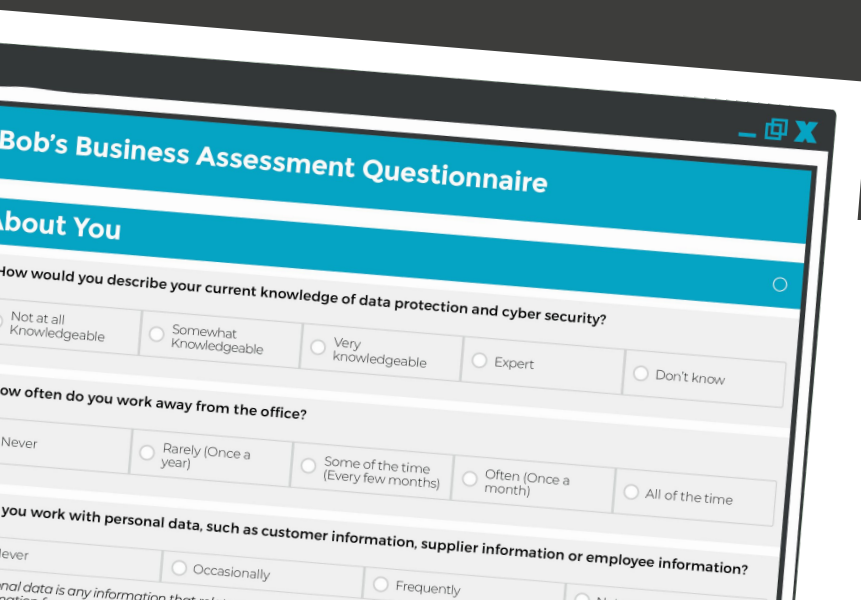
# Knowledge Assessment

- Assesses user knowledge on all key cyber security topics relating back to all of our 24 modules
- The assessment will identify gaps in overall organisational cyber security knowledge and point out where training should be prioritised
- Training will then be targeted to the least knowledgeable topics and weakest areas



# Confidence Assessment

- Assesses user's overall confidence in their general cyber security practices.
- The assessment measures whether the organisation is overconfident, underconfident or have confidence matched to their level of ability.
- The reported confidence level is compared to the user's actual ability to see if confidence levels match up or if the organisation is displaying a risky level of confidence.



The image shows a screenshot of a web-based questionnaire titled "Bob's Business Assessment Questionnaire". The form is displayed on a device screen, with a blue header bar containing the title. Below the header, the section "About You" is visible. The first question is "How would you describe your current knowledge of data protection and cyber security?", with radio button options: "Not at all Knowledgeable", "Somewhat Knowledgeable", "Very knowledgeable", "Expert", and "Don't know". The second question is "How often do you work away from the office?", with radio button options: "Never", "Rarely (Once a year)", "Some of the time (Every few months)", "Often (Once a month)", and "All of the time". The third question is "How often do you work with personal data, such as customer information, supplier information or employee information?", with radio button options: "Never", "Occasionally", "Frequently", and "All of the time". The form is partially obscured by a dark grey overlay on the right side of the image.

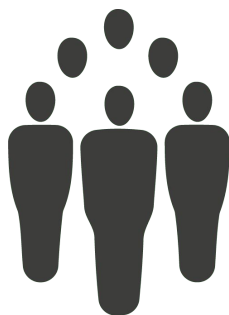
# Attitude Assessment

- Provides an overview of the organisational attitude towards cyber security.
- A more positive attitude suggests staff are more inclined to adopt cyber-secure behaviours. A negative attitude towards cyber security is associated with higher levels of risky cyber security behaviours.
- Attitudes are measured against the user's actual behaviour to identify whether users' reported attitudes match up against how they act in real life.



# Behaviour Assessment

- Assesses users' risky cyber security behaviours and provides an organisational measurement of risky cyber security behaviour.
- Reported behaviours are compared against user's actual behaviours to see if those that report to carry out a low level of risky behaviours are actually low risk users or not.
- Users' are more likely to fall victim to an attack when displaying a high level of risky cyber security behaviour.



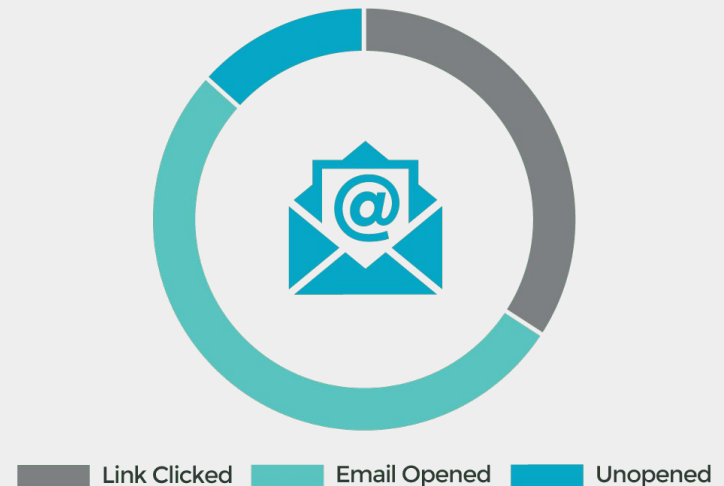
# Phishing Belief Assessment

- Measures user perceptions of how many phishing emails they receive.
- High risk users are those whose estimates differ greatly from the rate reported by the organisation. Much lower estimates indicate users not recognising phishing emails, while higher estimates may indicate users disregarding legitimate emails, or not reporting phishing emails to the IT team.



# Phishing Vulnerability Assessment

- Provides an indication of how vulnerable users think they are to phishing emails
- Reported vulnerability scores are measured against users' actual phishing vulnerability through the simulated phishing campaign
- An organisation where it's users perceive themselves not to be vulnerable to phishing, but are clicking on phishing emails frequently, are at a more significant risk





# Phishing Suspicion Assessment



- Provides a view of users' general beliefs about emails and how suspicious they are of emails being phishing emails.
- This allows for identification of risky behaviours such as those with a low level of suspicion
- A low level of suspicion means users' have less reason to question an email's legitimacy and so are more likely to fall victim to phishing. The higher the level of suspicion the better, as users are less likely to trust emails in general and are more likely to question the legitimacy of emails

# Phishing Optimism Assessment

- Measures user's confidence in their own ability to identify a phishing email, compared to a colleague's ability
- This will provide an overall organisational score of optimism
- Highly optimistic users underestimate their likelihood of being the target of a phishing attack. They are less likely to behave cautiously towards suspicious emails, and are at higher risk of being victim to phishing attacks



# Risk Assessment

- Measures user's confidence in their own ability to identify a phishing email, compared to a colleague's ability
- This will provide an overall organisational score of optimism
- Highly optimistic users underestimate their likelihood of being the target of a phishing attack. They are less likely to behave cautiously towards suspicious emails, and are at higher risk of being victim to phishing attacks



# About Bob's Business

Founded in 2007 by Melanie Oldham, Bob's Business was launched to mitigate the risk which makes all organisations susceptible to cyber security breaches - their workforce.

Today, Bob's Business is a leading provider of scientifically-informed cyber security awareness training and phishing simulation, working with organisations across the private and public sector to educate staff, transform cultures and deliver meaningful change.

## Get in Touch

Call us:

+27 (0)10 822 7392

Email us:

[sales@sovaton.com](mailto:sales@sovaton.com)

Book a web demonstration:

[sales@sovaton.com](mailto:sales@sovaton.com)

