PURECLOUD

CYBSAFE // WHITEPAPER

Behaviour Change:

AN INTELLIGENT APPROACH FOR CYBER SECURITY

Dr. John Blythe, CPsychol,
Head of Behavioural Science

Oz Alashe MBE
CEO & Founder

www.cybsafe.com

TABLE *of* CONTENTS

About CybSafe Research and Analysis

We know what works and what doesn't when it comes to behaviour change.

Our behavioural scientists have been designing and delivering behaviour change for nearly a decade. Dr John Blythe, our Head of Behavioural Science, is a Chartered Psychologist with the British Psychological Society and a Honorary Fellow at the UCL Dawes Centre for Future Crime. He brings over eight years experience exploring human aspects of cyber security having worked in academia, government and industry.

At CybSafe, we're building a future that reshapes the way organisations approach human cyber risks. We are one of the few organisations of our type with a dedicated behavioural science team focused on research and analysis

Understanding the science of human behaviour is key to this vision and our Research and Analysis work is based on three key principles:

1. Insights and best practice from **psychology** to change behaviour
2. **Scientifically evaluated** to know what works in changing behaviour and why
3. **People-centric** so that people are both productive and secure at work

Our product is developed and maintained through research and in collaboration with world-renowned academic research partners. We want to protect people online by building the best product we can but also contribute to academic knowledge and government policy. Only through collaboration and policy impact can we help to address the wicked problem of cyber security and keep people, businesses and nations safe online.

Collaborations & Partnerships

UCL

UNIVERSITY OF BATH

University of BRISTOL

Northumbria University NEWCASTLE

University of Kent

BU Bournemouth University

National Cyber Security Centre a part of GCHQ

Department for Culture Media & Sport

Tackling the Human Aspect of Cyber Security: The need for effective behaviour change

> *Mark Watson is an administrator for a large bank, having worked there for over 10 years, one of his primary responsibilities has become transferring funds between different clients, partners and accounts. One afternoon, Mark received an urgent email from one of his superiors requesting an immediate transfer of funds to a specific client's bank account. Mark, sensing the urgency and severity from his superior's email, quickly sent the funds as requested. In the morning, Mark brought up the transfer with his superior only to be met with a blank stare and a confused look.*

In this scenario, Mark has just fallen for a spear phishing attack, and at all steps in this interaction, he has unknowingly contributed to a security breach by sending money to a criminal. To prevent this breach, or any security breach, happening again, the behaviours that cause them need to be identified and changed. It's a common misconception that cyber security is all about technology. Technology is obviously a massive part of cyber security, but alone it is not enough to protect you from modern cyber threats. Cybercriminals regularly exploit the human element and by focussing on changing people's behaviour, cyber resilience can be achieved.

Behaviour change is a challenge. People are creatures of habit and influencing, let alone changing their behaviour is hard and complex. But we believe it's a challenge worth tackling because in doing so we can help people protect themselves online, offline, at home and at work.

Changing behaviour requires intervention but why do so many attempts fail? In most cases, it's because they are misguided and only "skin deep"; they do not start by addressing why people aren't cyber secure in the first place. It is akin to a doctor trying to cure a fever with paracetamol but missing the patient's gangrenous leg, the actual source of infection and fever.

Addressing why people aren't cyber secure may seem simple and intuitive but it's in the area of simplicity that most approaches fail. The reasons behind reusing passwords are very different to those that make someone fall for a phishing bait and thus require different interventions to change behaviour.

As people, we often have ideas and theories about what will work when trying to change behaviour. Think about how often you give your friends advice when they are trying to reach a goal like keeping fit, quitting smoking or drinking less. We have ideas about what will work - "download this app", "follow this person on instagram", "keep a diary". These might be viable solutions but often they are not scientifically grounded and in many cases unlikely to change behaviour. We see this problem time and time again with awareness and behaviour change campaigns and training material for cyber security. Too many are built around false assumptions on what will actually change behaviour. But this doesn't need to be the case. **There is a science to behaviour change and it's the ingredient that's often missing.** Psychology and the behavioural sciences bring us over 40 years of research on *what works* in changing behaviour and *why*. At CybSafe, behavioural science is at the heart of everything we do, from product design to evaluation.

In this report, we outline the CybSafe approach to applying behavioural science, how it's embedded in everything we do and how our products drive behaviour change in employees. To start with, we will cover the basics on the psychology of cyber security.

The psychology of cyber security: How to think about behaviour change

The COM-B system — a framework to understand behaviour

Awareness:

Physical & psychological ability

Decision Making:

Conscious & unconscious

Environment:

Physical & social

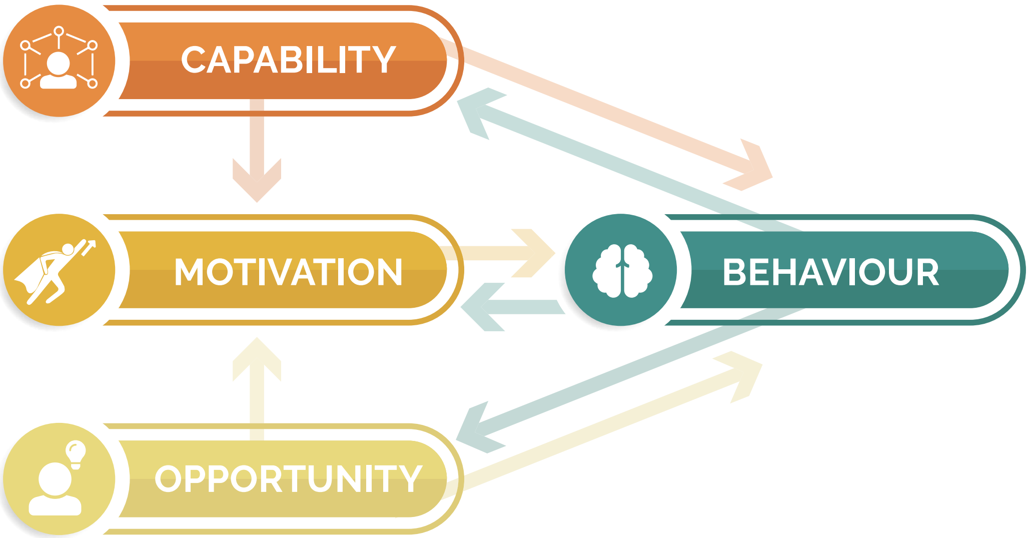


Figure 1. *The COM-B model of behaviour change*[1]

In order to change behaviour in a way that is sustainable, tailored, and targeted, we first need a thorough understanding of behaviour. We need to understand why behaviours are as they are and what needs to change for desired behaviour change. *Why do people download sensitive information to personal files? Why don't people use a VPN when working remotely? Why do people fall for phishing attacks?*

[1] Michie, S., Van Stralen, M. M., & West, R. (2011). The behaviour change wheel: a new method for characterising and designing behaviour change interventions. Implementation science, 6(1), 42.

Answering these questions requires understanding what is driving risky security behaviour. The COM-B model of behaviour was developed as a simple model of behaviour[1] change. It argues that behaviour is part of an interacting system of a person's capability, opportunity and motivation. Encouraging a person to change their behaviour requires changing one or more of the COM-B components.

CAPABILITY is a person's psychological and physical capacity to do a behaviour. In cyber security, we often refer to this as awareness (such as having knowledge of cyber risks) but a lack of capability may also be connected to a person's skills (such as password creating, detecting phishing indicators), memory and attention processes (such as remembering passwords) and lack of self-regulation (inability to follow through with goals or intentions).

OPPORTUNITY is anything that makes being secure possible or impossible, that lies outside the person. Opportunity is both physical and social. Physical opportunity consists of environmental factors like computer resources, security policies and physical restrictions. We know that when security doesn't work for people, it doesn't work[2].

We also know that security needs to be usable for people to engage with it yet physical opportunity is still the most overlooked component in cyber security and is a key reason why awareness campaigns alone fail. Opportunity is also more than just the physical environment, it is also the social environment, consisting of social and cultural influences on behaviour, such as social pressure from peers and management in the workplace and the organisational culture around cyber security.

[2] NCSC (2017). People: The Strongest Link. Presentation by Emma W, Available: https://www.ncsc.gov.uk/information/people-strongest-link

MOTIVATION is anything that energises and directs behaviour. It is like the head and the heart; people are either slow/rational (head) in their thinking or fast/automatic (heart). Although people like to think they make rational decisions all the time, mostly it's the "heart" that's driving the decisions that make our actions irrational. These fast decisions are subject to a mass of mental shortcuts and biases. There are hundreds of biases that we rely on, they help to speed up the vast array of information we process daily but they can also lead to undesirable behaviour (such as opening attachments we know we shouldn't or clicking on links instinctively). For example, we tend to listen to information that confirms our preconceptions - a shortcut referred to as *confirmation bias*, or we are overly optimistic regarding our ability to be cyber secure - a shortcut referred to as *illusory superiority bias*.

The COM-B model demonstrates the important conditions that are required to perform any behaviour and is an overarching summary of hundreds of psychological theories. The simplicity of the model is reflected throughout frameworks, policies and even legal systems.

In the US, to prove one's guilt in a criminal trial you need to show that the offender had the means (capability), motive and opportunity to commit the offence (behaviour). Whilst simplistic, the model is really useful to think about when analysing people's cyber security behaviour and trying to think about where to intervene.

In the next section, we show how we use the understanding gained from such models to design behaviour change interventions.

The CybSafe Method: From human cyber risks to human cyber resilience

We use a three-stage iterative process here at CybSafe.

Stage 1: Understand

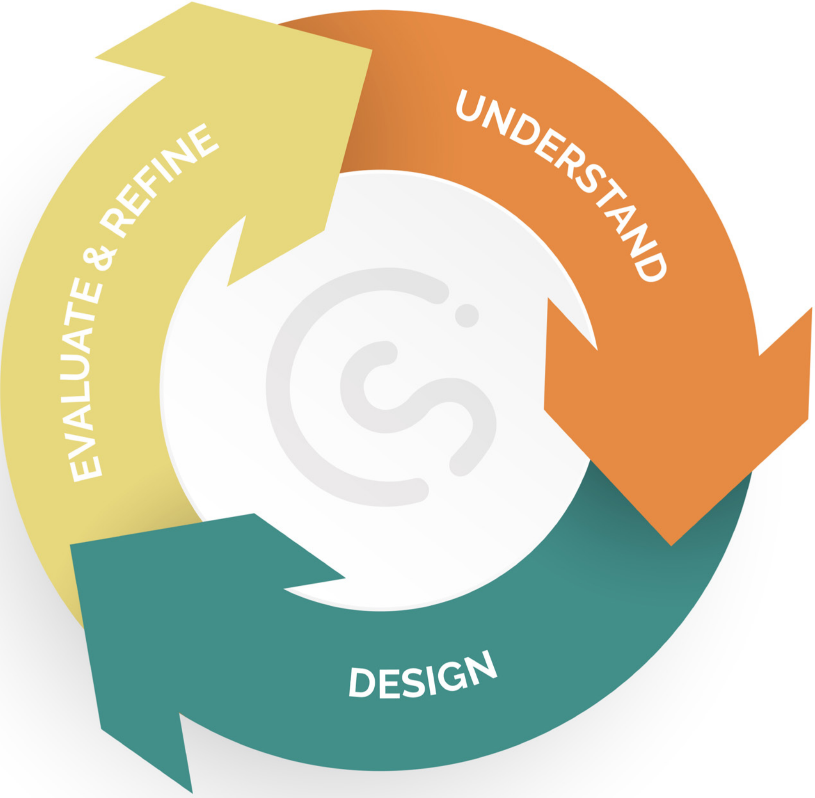
- COM-B
- Evidence-base (literature reviews & deep dives)

Stage 2: Design

- Behaviour change wheel
- Intervention strategies
- Modes of delivery
- Designing for engagement
- Behaviour change techniques
- User stories
- Interface design
- UX

Stage 3: Evaluate & Refine

- Impact assessment
- Metrics
- A/B Testing
- Randomised Control Trials (RCT)



⊙ Stage 1: Understand

We start by gaining insight into the behavioural problem using behavioural science models and frameworks, the evidence base, and through additional inquiry with users.

⊙ Stage 2: Design

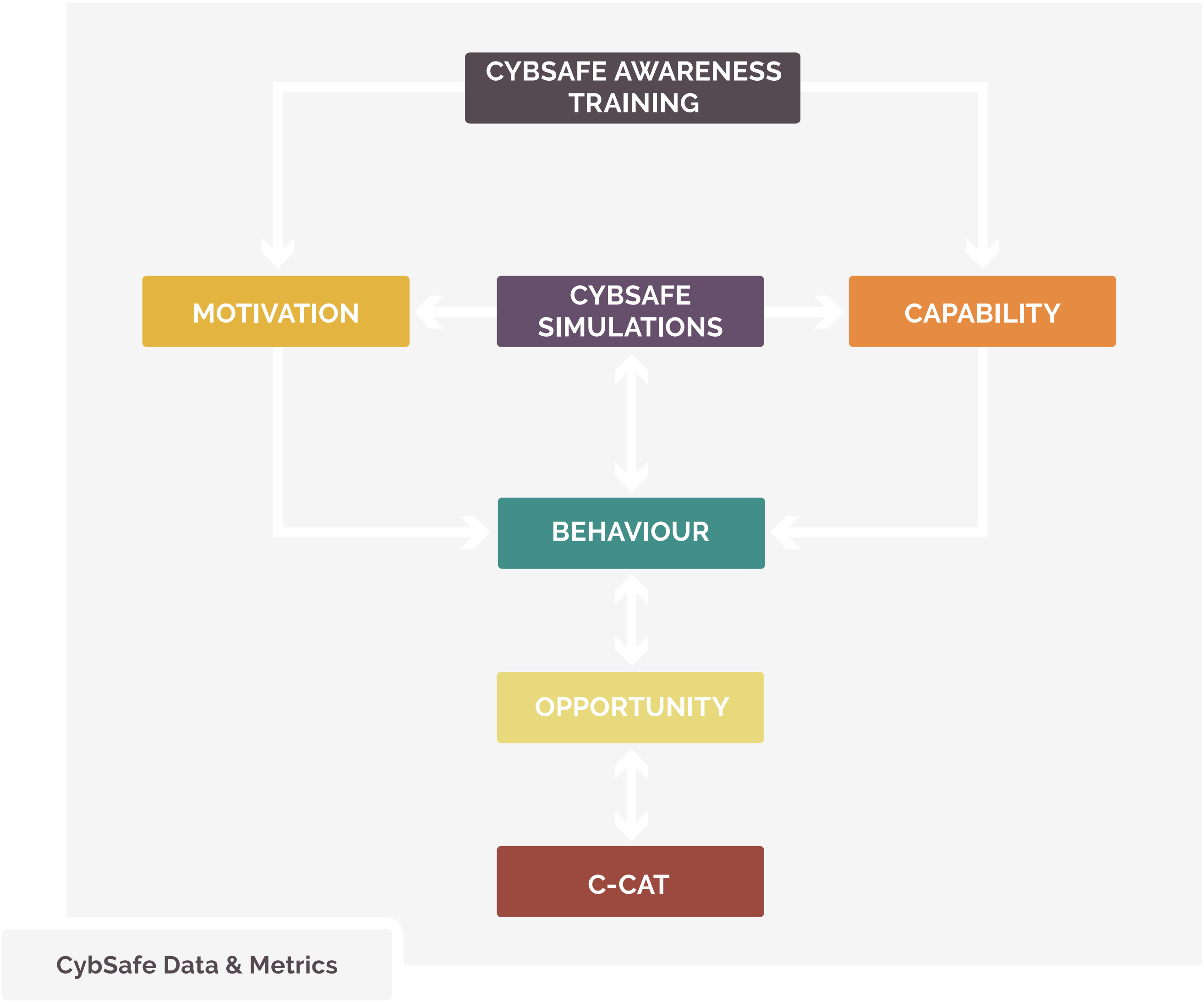
Based on our analysis, we then design the intervention through the selection of appropriate intervention techniques. There are over 90 techniques for delivering changes in either capability, motivation or opportunity and different techniques are more effective for different components[3]. These techniques can range from giving feedback on behaviour, giving information on cyber risk consequences to creating feelings of anticipated regret (raising awareness of expectations of future regret about unwanted behaviour) and habit formation. During this stage, we also optimise the user experience by implementing our techniques creatively and designing for user engagement.

⊙ Stage 3: Evaluate & Refine

Evaluation is an essential part of cyber security behaviour change interventions and helps to determine *what works* in changing behaviour and *why*. Answering this helps us to optimise and improve interventions, enhance user engagement and amplify behaviour change impact. Without examining effectiveness, it is also not possible to show value for money, justify content, or demonstrate that the intervention had the desired effect. Data science and cognitive computing technology provide significant advantages here enabling us to derive insight and understanding from mass data points whilst automating the refinement process so that users benefit in real time.

[3] Michie, S., Richardson, M., Johnston, M., Abraham, C., Francis, J., Hardeman, W., ... & Wood, C. E. (2013). The behavior change technique taxonomy (v1) of 93 hierarchically clustered techniques: building an international consensus for the reporting of behavior change interventions. Annals of behavioral medicine, 46(1), 81-95.

Behaviour Change: The CybSafe Way



The diagram above shows how CybSafe provides insights and drives changes in capability, opportunity and motivation.

- **CybSafe Awareness Training** focuses on enhancing employees' capability and motivation by using various intervention techniques.

- **CybSafe Culture Assessment Tool (C-CAT)** is our comprehensive tool that allows organisations to measure and improve their people-centric cyber security culture. C-CAT assesses the social and physical opportunity of people's engagement in cyber security, providing further insight into how people interact with security at work and how your organisation enables or inhibits cyber security behaviour.

- **CybSafe Simulations** provide insight into the day to day cyber security behaviour of employees. They also provide *teachable moments* by telling people when they have fallen for a phishing attack and reminding them of what to look out for. This further enhances capability and motivation for those most at risk of falling for an attack.

- **CybSafe Data and Analytics Reports Dashboard** brings this all together and provides actionable insights, recommendations and evidence, helping you to further drive behaviour change. This may, for example, occur through environmental restructuring (e.g understanding what isn't working for your people), culture change, or developing people-centric security policies and procedures in your business.

ABOUT *the* AUTHORS

Dr. John Blythe, *CPsychol,*
Head of Behavioural Science

Dr. Blythe is the Head of Behavioural Science at CybSafe.

With a background and PhD in psychology, he

specialises in behaviour change and human aspects of cyber security.

John is passionate about helping organisations move towards a people-centric security culture and to develop awareness training that is grounded in behavioural science.

He has an extensive research background and has in the past led on a number of Government and industry funded projects exploring the intersection of behaviour change and cyber security. John has previously worked at the Department for Digital, Culture, Media, and Sport (DCMS), and both the Dawes Centre for Future Crime and the Centre for Behaviour Change at University College London. Alongside his academic publications, he co-wrote the government reports on "Using behavioural insights to improve the public's use of cyber security best practices" and more recently, "Secure by Design: Improving the cyber security of consumer Internet of Things" whilst at DCMS. He collaborates regularly with academics and policy-makers and holds an Honorary research position at the UCL Dawes Centre for Future Crime.

Oz Alashe MBE
CEO & Founder of CybSafe

Oz Alashe MBE is CEO and Founder at CybSafe, an innovative and fast-growing British cyber security company based at the prestigious Level39 tech community in Canary Wharf.

A former UK Special Forces Lieutenant Colonel, Oz is now focused on making society more secure by helping organisations effectively address the human aspect of cyber security.

He and his team have developed a software platform that leverages science, advanced data analytics and cognitive computing technologies to measure and improve cyber security awareness, behaviour and culture.

He has extensive experience and understanding in the areas of intelligence insight, complex human networks and the human component of cyber security risk. He is also passionate about reducing societal threats to stability and security by making the most of opportunities presented through advancements in technology.

Oz's dynamic and socially-driven mission approach means he is regularly asked to comment in the national press as well as speak at events, often talking about issues relating to intelligence, cyber security and the socio-tech challenges faced by society. He is also a keen advocate of social investment and has worked with several mentorship schemes and charities that aim to help young people from all walks of life fulfil their potential.

Oz was made an MBE in 2010 for his personal leadership in the most complex of conflict environments.

CLICK HERE **if you would like to hear more about CybSafe and how it helps you address the human aspect of cyber security risk.**

PURECLOUD