PURECLOUD

CYBSAFE // WHITEPAPER

Measuring Cyber Security Culture

AN INTELLIGENT AND SCIENTIFIC APPROACH TO PEOPLE-CENTRIC CYBER SECURITY CULTURE

Dr. John Blythe, CPsychol.
Head of Behavioural Science

Oz Alashe MBE
CEO & Founder

www.cybsafe.com

TABLE *of* CONTENTS

Introduction

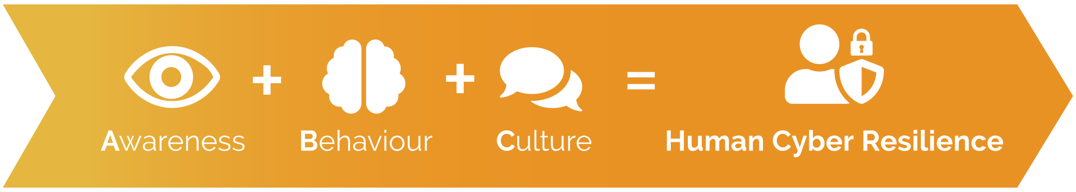
Most security awareness training attempts to raise awareness only. To decrease risk, security awareness training must raise awareness, change behaviour and build a culture of security.

It's an unfortunate fact, evident to both those who work in security and those who don't, that security awareness training in its current form isn't working.

Security awareness training is now a regulatory requirement in many industries. Even in industries in which it isn't, organisations large and small voluntarily invest in security awareness training in an effort to prevent data breaches. And yet data breaches are still commonplace – with human error often being either a cause or catalyst in the majority of breaches.

It's clear, and it has been for a long time, that traditional tick-box security awareness training efforts aren't working. And they're not working because they make little or no effort to change people's behaviour.

To reduce human cyber risk, security awareness training must go beyond raising awareness and should also focus on changing behaviour and building a culture of security simultaneously – together known as **'ABC'**.



Awareness + Behaviour + Culture = **Human Cyber Resilience**

Most security awareness campaigns focus only on awareness, the **A**. That's all well and good. But if raising awareness fails to change people's behaviour in practice (which is frequently the case), raising it becomes pointless. Awareness, as we know, is necessary but not sufficient for tackling human cyber risk.

It's for precisely that reason that more and more security insiders now believe it's only by addressing security awareness, behaviour and culture in tandem that human cyber risk can be reduced.

And yet, despite the rhetoric, most security awareness training shows little sign of doing so.

The moniker *"security awareness training"* has become misleading. It suggests that to increase human cyber defences, all we need to focus on is increasing security awareness – which is probably why tick-box training is still the accepted norm. Today, to those in the know, the definition of security awareness training has evolved.

To reduce your human cyber risk, it's important that your security awareness training focuses on advancing security awareness, behaviour and culture simultaneously. Doing so creates a virtuous circle in which improvements in one area flow into the next. Raising awareness lays the foundation for changes in behaviour. Secure behaviours nurture a culture of security. And, completing the circle, a culture of security advances awareness.

The ability to measure cultural alignment with organisational goals is becoming ever more important, and organisations that are unable to do so will lack a key component in the risk strategy.

In this whitepaper, we're excited to announce the introduction of the CybSafe Culture Assessment Tool (C-CAT). The next evolution in our approach to the **C** in ABC.

What is the CybSafe Culture Assessment Tool (C-CAT)?

C-CAT is a new and innovative tool that facilitates the measurement and development of a people-centric cyber security culture. Through a digitised diagnostic survey and data analysis engine, C-CAT reveals insights to help you direct and shape your culture using powerful analytics and behavioural science.

C-CAT has been developed by our in-house Behavioural Science team, led by BPS Chartered Psychologist Dr. John Blythe. It uses scientific principles to ensure that the tool is both valid and reliable (i.e. that it measures what it purports to measure and does so consistently). C-CAT focuses on seven key dimensions that have been scientifically proven to predict human cyber risk and behaviour.

The tool identifies the elements of your company that are supporting a people-centric security culture and the elements that are not. In doing so, it provides leaders with recommendations on how to develop and foster a people-centric security culture. These recommendations include clear metrics, giving leadership focused goals and the drive to make meaningful changes to culture.

This white paper details our work on people-centric culture, how we measure it and the scientific approach we have taken in its development.

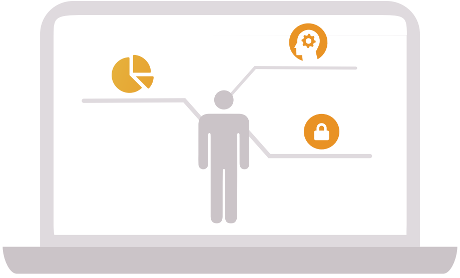
What is a people-centric cyber security culture?

Cyber security culture is a hot topic for many organisations at the moment, yet understanding, measuring and improving culture remains a time consuming and a difficult challenge. Often the cyber security messaging communicated through an organisation's stated values, strategies and policies does not reflect the way in which security is actually done in the workplace.

Understanding an organisation's security culture is an integral part of understanding its overall risk profile; it's possible, for example, for an individual to know what to do, to hold a positive attitude towards security and yet to behave in an insecure manner thanks to a corrosive culture of mistrust, individualism or unrealistic expectation.

In its simplest sense, culture can be described as *"the way things are done around here"* but culture means different things to different people. We focus on "people-centric culture" which we define as:

> *"A **focus on people:** the way they behave; what they really think about cyber security; and the things that encourage or prevent them from behaving securely as shaped through the organisation's physical and social environment."*



When companies have a positive cyber security culture, employees have a greater understanding and awareness of cyber security in the workplace and a commitment to behave in a secure manner.

Tackling security culture is a challenge as it is part of an organisation's wider culture and is shaped both formally and informally by many aspects of the organisation - from its mission and strategy to its practices, structures and communications, all the way to its building structures and floorplans. Companies also have subcultures which may differ by office, region and country. Attempts to change culture often fail because they try to retrofit a security culture to an existing culture. A security culture is more likely to take hold if it aligns with the grain of the current culture, rather than working against it.

There is also no single ideal security culture to which every organisation should aspire. An organisation in the United Kingdom will most likely differ from an organisation in the United States, and in a similar vein an organisation within the legal sector will differ greatly from an organisation within the healthcare sector. If culture is specific to an organisation, then how do you measure cyber security culture consistently across-and-within organisations?

Indeed, there is no one-size-fits-all when it comes to culture. However, regardless of the organisational or security culture you have, scientific evaluations can measure the extent to which you have a people-centric security culture and, in doing so, provide an evidence-based assessment on this aspect of human cyber risk for your organisation, as well as revealing clear ways in which you can reduce risk further and increase resilience.

For example, we know that security works best when policies and procedures do not impede productivity[1]. We also know that engagement, trust and collaboration with users is important[2] and having adequate resources and communications in place is necessary for engagement in security.

An organisation that focuses on these dimensions will have a stronger people-centric security culture than one that doesn't and, consequently, be more cyber resilient.

[1] https://www.ncsc.gov.uk/speech/people--the-strongest-link

[2] Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015) (pp. 103-122).

How to measure and shape culture?

Identifying how an organisation performs on different cultural dimensions offers the opportunity to steer culture towards something more people-centric. Taking the time to assess an organisation's security culture at a granular level makes it possible to identify which aspects aren't meeting the desired standards, individual dimensions that need to be addressed and the single most appropriate course of action.

This is where the **CybSafe-Cultural Assessment Tool**, more simply **C-CAT**, comes in; a tool that allows organisations to identify their culture at a granular level with ease. C-CAT was developed as a response to the current gap in the fight against cybercrime, addressing the importance of culture through the use of a quick, engaging survey for people to complete.

CybSafe Culture Dimensions

Here are the seven dimensions measured by C-CAT. In the rest of the whitepaper, we outline our scientific approach to the development of C-CAT and the science behind these dimensions.

Trust	The confidence employees have in their organisation's cyber resilience.
Just & Fair	The extent to which employees feel fairly treated in regards to cyber security and comfortable enough to speak up when confronted with security-related issues.
Responsibility	The extent to which employees view cyber security as being their responsibility.
Resources & Communication	The quality and quantity of cyber security communication material and training received at work.
Productive security	The extent to which employees feel they can be both secure and productive at work.
Ease & Choice	The levels of comfort and confidence employees' have when interacting with cyber security.
Community	The perceived level of social acceptance towards security-related behaviours.

C-CAT Features

Culture Insights & Segments

Understanding and interpreting culture isn't always easy, but C-CAT delivers cultural insights through simple charts and diagrams. With C-CAT, you can see which cultural dimensions deserve the lion's share of your attention in a single glance.

C-CAT's user-friendly interface also allows you to view cultural insights at different levels. You can check the cultural health of an organisation in its entirety, compare different departments or groups and take a deep dive to explore individual cultural dimensions.

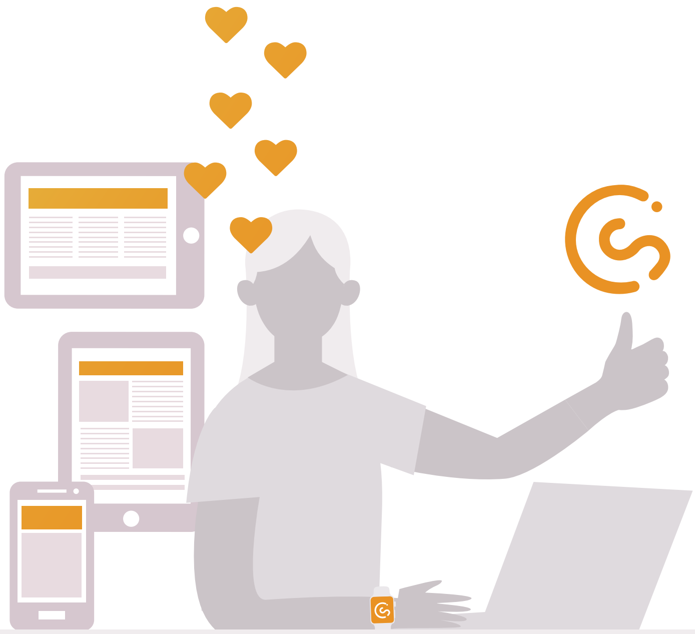
Charts also show how your organisation is performing compared to industry benchmarks. This allows you to benchmark against organisations of the same size, industry or geographical location, for example.

Focus Recommendations

Focus recommendations are provided alongside charts depicting culture insights, and immediately highlight both strong and not-so-strong cultural dimensions. Recommendations facilitate the construction of specific interventions individually tailored to the needs of your organisation.

Assess, Improve and Track

To check that awareness, behaviour and culture interventions are working, culture can be measured and monitored repeatedly and insights are consistently updated and adjusted over time.



Scientific Approach

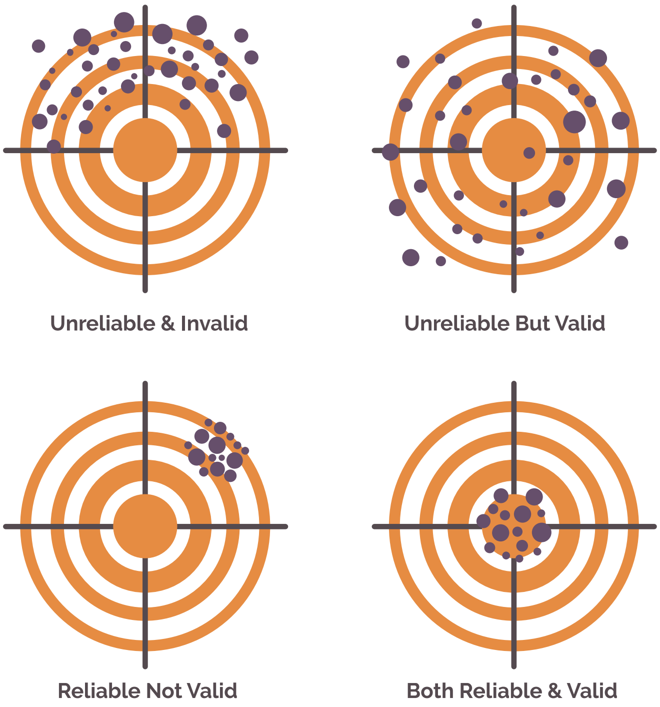
At CybSafe, we have taken a scientific, rigorous approach to the creation of C-CAT to corroborate the framework's reliability, validity and scientific grounding. Our approach, spearheaded by BPS Chartered Psychologist Dr. John Blythe, more than hints at culture: it guarantees accurate people-centric cultural identification.

As culture dimensions are relatively abstract (i.e. they cannot always be directly observed), the greatest challenge is measuring them in a reliable and valid way through surveying the employees of an organisation. Reliability and validity are the two key criteria in determining the quality of any survey that seeks to assess a phenomenon (such as culture).

- **Validity** - derived from the latin meaning strong. It is the degree to which the survey measures what it claims to measure. Validity is a necessary measurement because it helps to determine that a tool is cost-effective, ethical and truly measures what it claims to measure.

- **Reliability** - is how consistent the tool is. A tool with good reliability will produce similar results under consistent conditions.

The following diagram illustrates the importance of validity and reliability in accuracy.



Unreliable & Invalid

Unreliable But Valid

Reliable Not Valid

Both Reliable & Valid

C-CAT was developed by our Research & Analysis team (led by Dr. John Blythe, a Chartered Psychologist with the British Psychological Society). To ensure that the tool was both valid and reliable, development followed scientific conventions outlined in academic literature[3] and international standards[4].

C-CAT was developed in three key stages:

STAGE 1: Literature Review

Prior to developing questionnaire items for the survey, we first conducted a literature review on cyber security culture and the facilitators and barriers to employee's cyber security behaviour. From this, we were able to identify key dimensions that have been scientifically demonstrated to be important for driving cyber security behaviour in employees.

STAGE 2: Survey Item Generation and Reduction

Of the dimensions identified in the literature review, we developed a preliminary suite of questions designed to facilitate dimension measurement. We piloted our suite with subject-matter experts who determined whether each individual item was (i) conceptually consistent and adequately measured the intended dimension and (ii) had good comprehensibility and clarity for the target population.

A well-designed survey requires reducing measurement and response bias. A well-known concern with surveys is that respondents will answer dishonestly, particularly when questions relate to aspects of their job performance. Feelings of repercussion or embarrassment are just some of the reasons why people answer surveys dishonestly. This

[3] E.g. Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. Organizational research methods, 1(1), 104 121.

[4] E.g. EFPA test review criteria - http://www.efpa.eu/professional-development/assessment

phenomenon is known as social desirability bias
- the tendency for people to answer questions in a manner that will be viewed favourably by others.

We have reduced the tendency for people to give biased responses by designing C-CAT using privacy-by-design principles. Employee responses on C-CAT are anonymous and confidential - so that employees can give honest answers about their organisation's culture without fear of repercussion. We also deployed dependable statistical processes to identify and discard questions that elicited socially desirable responses[5].

A further challenge is that respondents often suffer from survey fatigue when answering surveys - becoming tired and providing low quality responses (e.g. selecting the same response for all questions). This is particularly the case when surveys are lengthy and time consuming.

C-CAT was designed to be short. C-CAT can be completed in less than five minutes, reducing the likelihood of respondent fatigue.

A final potential C-CAT response bias is acquiescence bias - the tendency for people to agree with all the questions on a survey. To overcome this, we have enlisted a number of data checks such as using a balance of positively and negatively keyed items, calculating an average completion time and removing extreme outlier responses that may impact on the quality of the data.

STAGE 3: Reliability and Validity Assessment

Finally, we piloted C-CAT with a large sample to reduce and refine the tool and to further evaluate the instrument for reliability and validity.

[5] Hays, R. D., Hayashi, T., & Stewart, A. L. (1989). A five-item measure of socially desirable response set. Educational and psychological measurement, 49(3), 629-636.

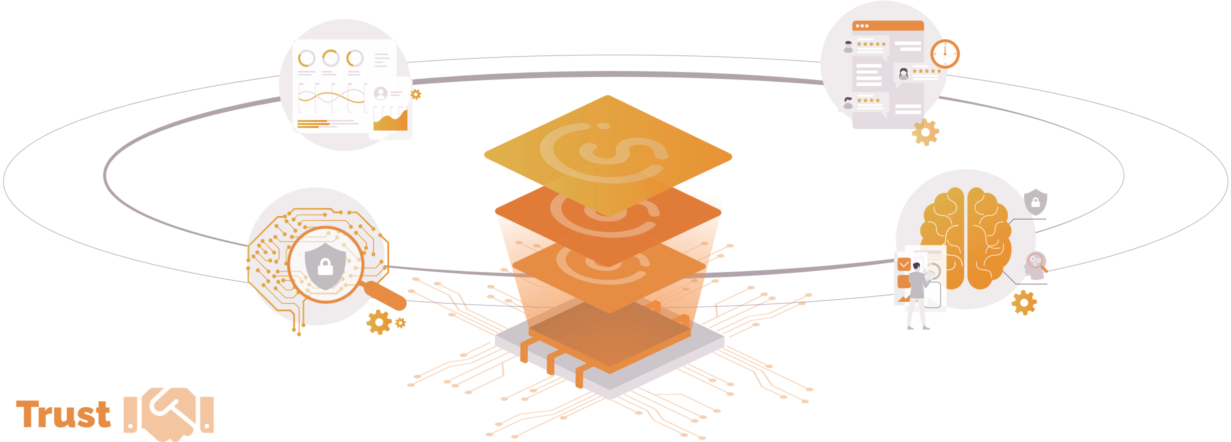
Validity - Using statistical analyses (exploratory and confirmatory factor analyses) we found that there was a seven-dimension structure for culture demonstrating that the tool had good construct validity[6]. We also assessed the extent to which the survey measured our outcome of interest: cyber security behaviour, finding the seven-dimension structure significantly predicted engagement in cyber security behaviour[7].

Reliability - We assessed the internal reliability of our survey and found that the survey had high reliability (cronbach's alpha=.87) We also reduced the survey to final set of 27 items measuring 7 cultural dimensions. These three stages allowed us to produce a cultural assessment and improvement tool that has strong scientific rigour and meets globally recognised standards.

[6] The degree to which a test measures what it claims, or purports, to be measuring.

[7] A multiple linear regression was calculated to predict cyber security behavior based on the seven cultural dimensions. A significant regression equation was found $F(7,423)=20.492$, $p<.001$), with an R^2 of .225.

The science behind our dimensions



Trust

Trust is an important dimension within security culture, as employees need to have faith in both the processes in place and the individuals who put the processes in place if employees are to follow the processes. If there is a feeling of uneasiness or mistrust towards the choices of an organisation then it's unlikely that the appropriate behaviours will be maintained[8].

Trust also needs to work both ways. Reciprocal trust between staff and the organisation is essential for effective engagement with cyber security[9]. Often, employees are monitored heavily and their behaviour is restricted excessively. Research shows such an approach to be questionable.

[8] Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & security, 31(4), 597-611; Blythe, J. M., Cove try, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In Eleventh Symposium O unable Privacy and Security ({SOUPS} 2015) (pp. 103-122); Kirlappos, I., & Sasse, M. A. (2015). Fixing Security Together: Leveraging trust relationships to improve security in organizations. Proceedings of the NDSS Symposium 2015, (1), 1–10 https://doi.org/10.14722/usec.2015.23013

[9] ENISA (2018). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity; Kirlappos, I., & Sasse, M. A. (2015). Fixing Security Together: Leveraging trust relationships to improve security in organizations Proceedings of the NDSS Symposium 2015., (1), 1–10. https://doi.org/10.14722/usec.2015.23013

Indeed, according to the literature[10], security leaders are more likely to advance cyber security by incentivising trustworthy behaviour in employees rather than restricting and controlling their actions. It seems as though employees who feel trusted and supported are motivated to behave securely[11]. As the National Cyber Security Centre note, trust takes time to build because if people think they will get into trouble, they won't behave securely[12].

Just and Fair

A Just & Fair culture is integral to security culture as it emphasises shared security accountability between leaders and staff. In turn, shared accountability ensures breaches are reported as and when they occur, which allows organisations to limit damage and learn from mistakes. Not only do employees need to trust in the competence and decision making capabilities of their organisation, but they need to feel confident and comfortable enough to speak up when confronted with security issues or a suspected security breach. Clearly, employees that are unjustly monitored or blamed for security-related issues are incentivised to keep quiet when issues arise.

Rejecting the idea of blame being a useful concept is an important step towards cyber resilience within organisations, but too often people are blamed for their inability to follow cyber security and people are thus denounced as the "weakest link" in security. To create security "pillars", rather than "weak links", people need to be engaged in security and this requires investment in a workplace environment that encourages positive security acts rather than an environment that blames, bullies and punishes people for being human[13].

[10] ibid.

[11] ibid.

[12] https://www.ncsc.gov.uk/collection/you-shape-security

[13] Reason, J. (2017). The human contribution: unsafe acts, accidents and heroic recoveries. CRC Press.

Resources and Communication

Resources & Communication is another dimension fundamental to fostering a strong security culture. That's largely because the Resources & Communication dimension is positively associated with awareness. Better resources, communication and education advance awareness[14], and security awareness is one of the cornerstones of a resilient organisation.

By providing employees with security-related communications and material, awareness can be increased and a strong security culture can be bolstered. Specifically, it is important to provide employees with contextualised material that is specific to their role, industry and level of experience, so that they are aware of the actual threats that could be posed to an individual in their position[15]. Organisations may use a variety of modes to deliver their awareness content, such as posters, desk drops and face-to-face training.

Further, it's been suggested that strain and stress in the workplace arise as a result of an imbalance between the demands of a task[16] and the resources available to help tackle said task. Workplace resources, for example, might include training, access to IT support, clear communications and autonomy; all help employees which learn, grow and tackle any challenges or demands[17]. Should an employee be asked to follow complex security policies

[14] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237-248.

[15] Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations. Information Management & Computer Security, 22(4), 334 345.

[16] Bakker, A. B., & Demerouti, E. (2007). The job demands-resources model: State of the art. Journal of managerial psychology, 22(3), 309-328.

[17] Wang, Y., Huang, J., & You, X. (2016). Personal resources influence job demands, resources, and burnout: A one-year, three-wave longitudinal study. Social Behavior and Personality: an international journal, 44(2), 247-258.

without appropriate training, the chasm between the demands of the task and the resources available to help complete the task can cause undue and undeserved strain and stress. Resources & Communication is therefore central to a healthy security culture.

Productive Security

Productive Security also contributes to an organisation's security culture, as it has been shown that security policies designed to aid productivity are more likely to be followed. Sadly, security policies are often developed without fully understanding how people work in organisations. Such security policies prohibit productivity. And, because people's mental resources are limited, such security policies force employees to make a choice. They can either follow the policies and crawl through their to-do lists at a snail's pace, or they can shape security policies around their existing responsibilities.

In fact, research shows that people routinely craft their own versions of security policies when official policies are cumbersome and poorly implemented. If employees feel like they can't be secure and productive at the same time, then it's likely that organisational security policies need some work[18]. The NCSC in the UK refer to this as "you shape security" - a collaborative process to develop productive and secure policies[19]. Productive security requires integrating good security habits into the business processes.

[18] Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "Shadow Security": Why under standing non-compliance provides the basis for effective security. In NDSS Workshop on Usable Security (USEC).

[19] https://www.ncsc.gov.uk/collection/you-shape-security

Responsibility

Collaborative security efforts – efforts that span the entirety of a workplace – can prevent more cyber threats than solo attempts at threat prevention. To that end, responsibility has been deemed an important dimension contributing to security culture, as research has shown that the most at risk employees often delegate security to another source. This other source can be something technological, such as the assumption that an antivirus will block all attacks, or it can be another person or department within the organisation[20]. In fact, it has been shown that employees often delegate responsibility to one of four modalities: technology, individuals, organisations and institutions[21].

In any case, when employees delegate responsibility for security to others, there is a sense of resignation; a feeling that those "delegating" will never understand cyber security. With this resignation comes low confidence, which severely hinders any chance of a change in behaviour[22].

Ease and Choice

Related to individual behavioural control, Ease & Choice refers to the extent to which an employee feels at ease when performing a task. Research indicates that those who feel comfortable performing a task are likely to continue doing it, while those who struggle are likely to stop[23]. Kahneman[24] has suggested a variety of methods and steps we could take to provide "cognitive ease" and reduce "cognitive load".

[20] Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue, IT Professional, 18(5), 26-32.

[21] Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015) (pp. 103-122).

[22] Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. ICIS 2005 proceedings, 31.

[23] Terry, D. J., & O'Leary, J. E. (1995). The theory of planned behaviour: The effects of perceived behavioural control and selfefficacy. British journal of social psychology, 34(2), 199-220.

[24] Kahneman, D., & Egan, P. (2011). Thinking, fast and slow (Vol. 1). New York: Farrar, Straus and Giroux.

For example, repeating an experience or behaviour increases cognitive ease by making it feel familiar. Within cyber security, this could involve employees practicing reporting potential breaches periodically, so that the process feels familiar and easy. In a similar manner, the Behavioural Insights Team[25] has indicated that if you want to encourage a behaviour, then "make it easy": provide simple messages and reduce the hassle of taking up a behaviour.

Community

Finally, the role of Community is important in determining a security culture as social norms represent acceptable group conduct around security, i.e. social norms guide behaviour in organisations and act as rules depicting what people should do to protect data and information systems. A wealth of research has shown that a primary driver of behaviour is whether or not an individual believes other people they consider to be important approve of it[26]. These important people may be their immediate colleagues or line management but might also include personal contacts such as family and friends.

If people within an organisation feel like others will disapprove of security policy compliance (for example, if they feel they'll be looked down upon for sacrificing productivity in an effort to follow security policies), then security policies are unlikely to be followed[27]. Likewise, if people see others behaving in an insecure manner, it's probable they'll follow suit[28]. When it comes to organisational culture, management behaviour shapes the behaviour of employees. Closing the perceptual gap between leaders and staff helps ensure everyone focuses on the common goal: keeping the organisation secure[29].

[25] Team, B. I. (2014). EAST: Four simple ways to apply behavioural insights. Behavioural Insight Team, London.

[26] Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.

[27] Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. International. Journal of Information Security and Privacy (IJISP), 9(1), 26-46.

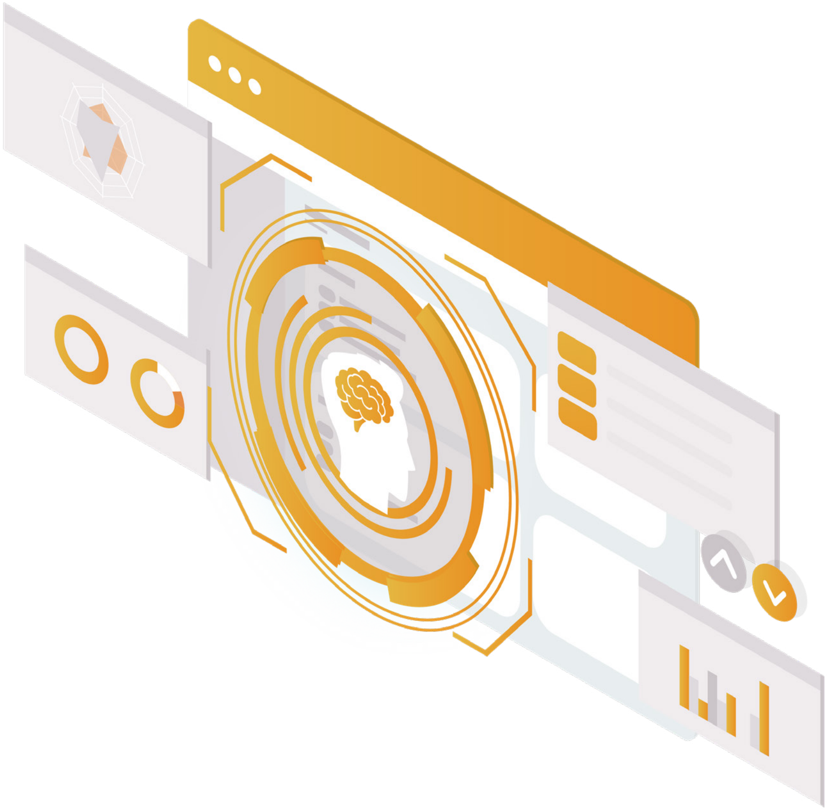
[28] Department for Digital, Culture, Media & Sport. (2018). Cyber Security Breaches Survey 2018. Retrieved from: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018

[29] Vogelsmeier, A., Scott-Cawiezell, J., Miller, B., & Griffith, S. (2010). Influencing leadership perceptions of patient safety through just culture training. Journal of Nursing Care Quality, 25(4), 288-294.

Conclusion

Building human cyber resilience is a difficult task. However, by focusing on the ABC (Awareness, Behaviour and Culture) of security, human cyber resilience can be developed. Culture is an important but often undervalued aspect of cyber risk.

We know that culture can be difficult to measure but C-CAT changes things. Through rigorous scientific testing, CybSafe has developed a tool that quantitatively identifies your organisation's strengths and weaknesses across seven cultural dimensions successfully proven to improve security behaviour.



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 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 advanced data analytics and cognitive 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 have attracted attention and interest from influencers and decision makers keen to address the realities of cyber security and the impact on people, business and community.

He is regularly asked to speak publicly, 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