



# Meaningful Metrics for Human Cyber Risk

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

**Joe Giddens**  
Head of Content, Concepts &  
Community

**Oz Alashe MBE**  
CEO & Founder

[www.cybsafe.com](http://www.cybsafe.com)



## // CONTENTS

Welcome!	3
<b>A BRIEF HISTORY OF METRICS</b>	<b>4</b>
At first, it was all about body parts...	4
<b>WHY ARE METRICS SO IMPORTANT?</b>	<b>5</b>
The tone at the top	5
<b>WHAT MAKES A METRIC “MEANINGFUL”?</b>	<b>8</b>
A “meaningful” metric	8
<b>MEANINGFUL METRICS FOR HUMAN CYBER RISK</b>	<b>10</b>
Measuring <b>A</b> wareness	11
Measuring <b>B</b> ehaviour	13
Measuring <b>C</b> ulture	19
<b>QUALITY AND IMPACT METRICS</b>	<b>22</b>
Quality metrics	22
Impact metrics	25
<b>CONCLUSIONS</b>	<b>27</b>
About the authors	28



# Welcome!

## To reduce human cyber risk, security teams need to respond to meaningful metrics

Today, we know that people influence cyber security. But most organisations fail to measure their human cyber risk.

Some measure security training uptake. Some go a little further and measure suspicious link-clicks or report-rates. But very few can answer key security questions:

**How has our human cyber risk changed over time?**

**How does our risk compare to that of our competitors?**

**Which security interventions reduce most risk?**

**Which provide the best ROI?**

To answer questions like this, we need **meaningful metrics**. We need to be able to benchmark. We need to be able to see progress. We need to be able to measure success.

**And we need to do more than just assess improvements in security awareness.**

In this paper, we discuss measuring security Awareness, Behaviour and Culture – meaningfully.

We also discuss how to measure the quality and impact of campaigns.

# A brief history of metrics



## At first, it was all about body parts...

People used to use their body parts to measure things. A foot, for example, was the length of a man's foot. An inch was the length of a thumb<sup>1</sup>.

Unsurprisingly, the method was problematic - the size of people's hands and feet vary greatly! And so, in around 500BC, the world's first abacus was born<sup>2</sup>. It was a monumental step forward. For the first time ever, humans had a standard form of measurement!

Soon we were measuring to our hearts content. Quantities, lengths, degrees; you name it. Over time, new measurement techniques spread. Then, in 1795, France adopted something called the "metric system"<sup>3</sup>.

## Present Day

Which brings us to the present. Today, "metrics" help us understand not just the physical world but also the digital world. "Mbps" measures internet speed. "Conversion rates" measure the share of people who take a desired action.

And metrics can help us understand and manage human cyber risk.

---

1 Moore, R. (1989). Inching toward the Metric system. *The American Biology Teacher*, 51, 213-218.

2 Stuijk, D. J. (1963). On Chinese mathematics. *The Mathematics Teacher*, 56, 424-432.

3 Halleburg, A. E. (1973). The metric system: past, present—future? *The Arithmetic Teacher*, 20, 247-255.

# Why are metrics so important?

## The tone at the top

The “tone at the top” shapes the cyber resilience of entire organisations<sup>4</sup>. It’s been proven many times over. Plus, today’s boards have a legal and moral obligation to manage cyber risk.

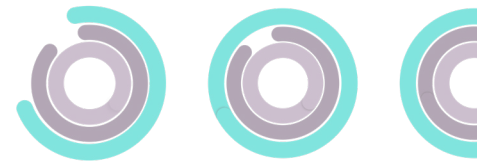
And yet today, 47% of FTSE 350 businesses believe cyber risk reporting is incomplete<sup>5</sup>.

**“Cyber security reporting at board level has grown from attempts to understand technology to the point where boards now have a fiduciary responsibility to manage cyber security risk.”**

Dave Padmos | EY Global Advisory Technology<sup>6</sup>

Nowhere is this more problematic than in the realm of human cyber risk. A lack of understanding, time and resources make it difficult to report meaningfully<sup>6</sup>. So we tend to focus on simple metrics like security knowledge<sup>7</sup>. But such metrics in isolation are poor predictors of human cyber risk<sup>8</sup>.

Worse, shaky metrics lead to shaky strategies. Take the classic “security knowledge” metric as an example.



<sup>4</sup> Roboff, G. (2016). The Tone at the Top: Assessing the Board’s Effectiveness. *ISACA Journal*, 6

<sup>5</sup> FTSE 350 Cyber Governance Health Check 2018

<sup>6</sup> Ernst & Young. (2018). EY Global Information Security Survey 2018–19. Retrieved from: [https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-201819/\\$FILE/ey-global-information-security-survey-2018-19.pdf](https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-201819/$FILE/ey-global-information-security-survey-2018-19.pdf).

<sup>7</sup> The Research Institute in Science of Cyber Security (2018). Analysis of Cyber Metrics Workshop. London, 23 May 2018. Retrieved from <https://www.riscs.org.uk/wp-content/uploads/2018/07/23-May-2018-Cyber-Metrics-workshop-analysis.pdf>

<sup>8</sup> Typically, comprehension is measured through online security test results delivered immediately after training – suggesting “comprehension” may in fact reflect little more than memory

<sup>9</sup> 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 (ISOUPSI 2015)* (pp. 103-122).

## Improving knowledge alone is not enough



Improving security knowledge is easy. All you need to do is drip feed people security advice. Then, you layer on more. And more still. The advice becomes niche. Advanced. Bulky. Irrelevant. But it improves people's "knowledge". So you continue.

Does the advice change people's attitudes for the better? Probably not.

Do behaviours advance? Who knows? (But probably not.)

When looking at the wrong metrics, we often miss what really matters<sup>10 11</sup>.

Couple this with the need to prove compliance.

You're focused on boosting security knowledge while achieving compliance. So you invest in dry, weighty "tick-box" security awareness training. After all, it meets both goals.

<sup>10</sup> Wertsch, J. (2001). The multivoicedness of meaning. In Wetherell, M., Taylor, S., Yates, S. J. (Eds.), *Discourse theory and practice: A reader* (pp. 222-235). London, UK: Sage.

<sup>11</sup> Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy?. *Computers & Security*, 39, 396-405.

## **To reduce human cyber risk, we must move beyond shallow risk metrics. We need to enlist meaningful metrics.**

The training and the misleading metrics suggest increasing security awareness reduces cyber risk. And, completing the circle, boards overlook the need to address human cyber risk.

There's more to human cyber risk than we currently appreciate.

Making good cyber security decisions requires data. Good data.

Data that we can present to decision makers knowing it's easy to understand.

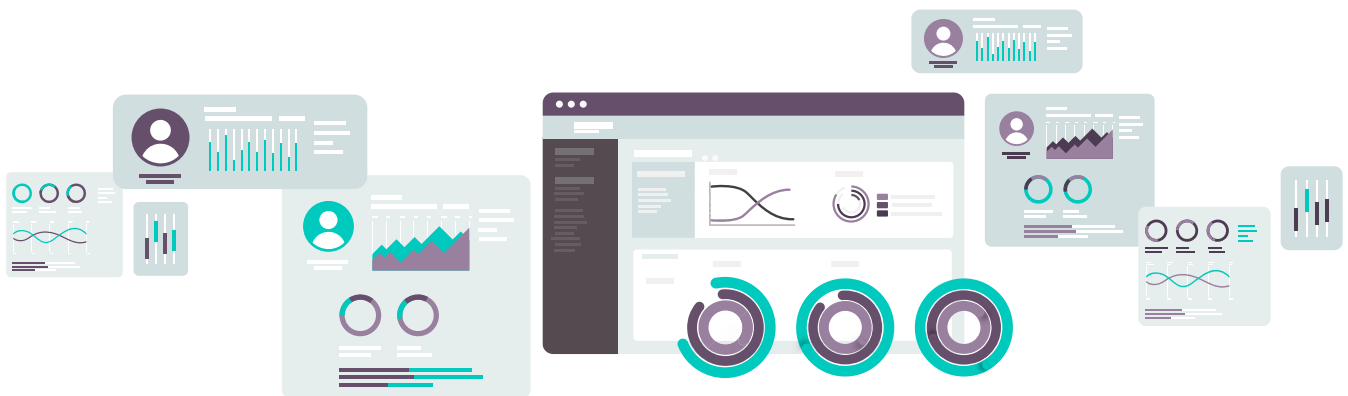
Which is what makes meaningful metrics so important.

CybSafe champions meaningful metrics.

We advocate using measurements, metrics, indicators and insights to highlight risks and opportunities. And we practise what we preach.

We measure using techniques that are evidence-based and scientifically-proven.

And we help and implore others to do the same.



# What makes a metric “meaningful”?

No single security metric can reveal the full spectrum of human cyber risk. To see cyber risk, we need to look at multiple metrics. All need to be “meaningful”.

What makes for a “meaningful” metric<sup>12</sup>?



## A “meaningful” metric:

- Is appropriate for its security goal. For example, password strength and exposure in data breaches measure password hygiene.
- Is simple and easy to interpret, understand, explain and act on.<sup>13</sup>
- Is benchmarked. For example, against the industry average.
- Is repeatable and reliable. Data checks should lead to the same result.

In contrast, a “bad” metric is difficult to understand. Bad metrics don't help with goal-setting. Nor do they aid decision-making.

When choosing metrics, make sure to use the SMART criteria to guide your choices.



## SMART criteria help with metric selection:

- **Specific:** Does the metric relate to a specific security goal?
- **Measurable:** Is the metric quantifiable? Or does it at least measure progress?
- **Actionable:** Can outputs shape future plans?
- **Relevant:** Is it relevant for your organisation and its risk profile?
- **Time:** Can you measure at different points in time?



## It's not all about the numbers

When thinking of metrics, we have a tendency to rely on measurements that provide numbers. People are comfortable with numbers. But it's important to also consider measurements and insights. And not just things that we can count.

Qualitative insights, such as interviews, focus groups and open-text employee feedback, are valuable. These types of insights can provide very rich data.

They may highlight opinions, sentiment, emotions, thoughts and feelings towards security. These are concepts that can often get lost if data is only summarised as numbers.

So, when thinking of "meaningful" metrics. Consider also gathering data that provides indicators and insights. To give context to what you are measuring.



# Meaningful Metrics for Human Cyber Risk

## Improving knowledge alone is not enough

Most security awareness campaigns focus on improving security awareness. That's all well and good. But if fresh awareness fails to change behaviour or culture, you have a problem. People's awareness improves. But their behaviour doesn't. Risky actions still offer criminals entry points. So you have greater security awareness. Yet human cyber risk remains unchanged.

Improving security awareness, behaviours and culture at once is a much better play. Improve all three at once and your human cyber risk falls.

To ensure you're improving, you need to measure:



First we discuss measuring security Awareness, Behaviours and Culture (ABC). Then we discuss measuring the success of ABC campaigns.

# Measuring Awareness

Awareness refers to people's knowledge and understanding about: cyber security risks; why these risks matter to the organisation and themselves; and the security behaviours required to reduce those risks.

Awareness interventions (comprising of education and training) will focus on ensuring that people know WHY security is important for them personally and their organisation, WHAT they need to do, and HOW to do it. Educational activity should increase knowledge or understanding, whereas training activity should impart skills and competence in people's ability to perform security behaviours.<sup>11</sup>

Awareness activities usually involve security communication, education and training. They include things like workshops, quizzes, and online training. All seek to enhance people's awareness of what to do, how to do it and why security is important.

Typically, awareness metrics measure "knowledge". They're usually collected on training completion. They measure only people's knowledge of the training provided.

For certain, the metrics show the efficacy of people's short-term memory. Do they do much more? It's impossible to say – which makes the metrics imperfect.



<sup>11</sup> Our definitions of Awareness, Behaviour and Culture were agreed by Academics and Industry using a Delphi Methodology

When it comes to awareness, you should measure two key areas:

## 1. The “what” and the “how”

- a. People’s **awareness of a threat**, as well as the **personal and organisational impacts** (what)
- b. People’s **awareness of their personal and organisational risk** (what)
- c. People’s **awareness of the behaviours and/or skills required to mitigate the threat** (how)

## 2. The “where” and the “who”

- a. People’s **awareness of help on offer**. Where and who can people seek support from? Help desks? Ambassadors? Share points? Internal policies?



### EXAMPLE

## CybSafe's Awareness Metrics

CybSafe awareness metrics show people’s security knowledge in a number of ways. These include things like:

- **The ability to recall the correct information to deal with cyber security situations**
- **The retention of knowledge over time**
- **The ability to combine individual pieces of information to solve multi-dimensional problems**
- **Understanding and awareness of organisational and personal threats (situational awareness)**

To track security awareness over time, we measure awareness periodically. And standardisation keeps metrics reliable across individuals and time.

## Measuring Behaviour

Security behaviours include all direct and indirect actions that influence cyber risk. Behaviour change refers to the likelihood of security behaviours being influenced.

Behaviours do not exist in a vacuum but occur within a context (such as the workplace or home environment) so organisations must be cognisant of the facilitators and barriers to behaviours that exist. Barriers to change prevent or make it difficult to enact security behaviours and include internal (such as mood, attitude and habit) and external (such as workload and time pressure) factors.

When it comes to behavioural metrics, you should measure two things:

1. The behaviours you're **hoping to change** or promote.
2. And – the part that's most often neglected – **why behaviours are happening** in the first place!

### Measure why a behaviour is happening

We'll come back to measuring behaviours shortly. Before we do, let's discuss measuring why a behaviour is taking place.

There's a reason this is so important:

When we fail to measure why a behaviour is taking place, the behaviour becomes very hard to change.

That's because when we're not measuring, we're assuming.



For example, we find out people are using weak passwords. We assume they're unaware of the risks. So we attempt to raise their awareness of the risks, assuming behaviours will change as a result.

That's a very big assumption.

A lack of security awareness isn't always the reason insecure behaviours take place. Poor cyber security behaviours persist even after "effective" awareness campaigns <sup>14</sup>.

Awareness might be necessary to change behaviour. But awareness in isolation is not sufficient. People go against security advice for all sorts of reasons.

## Why do people ignore security advice?

Common reasons include:

- **Underestimating their chance of becoming a victim.**
- **Overestimating their ability to respond to security threats.**
- **A maxed-out compliance budget. (We all have a limited amount of mental effort we can call on. When security demands too much mental effort, we take risks.)**
- **Low confidence in security skills.**
- **Environmental factors (such as policies mandating monthly password changes).**

---







<sup>14</sup> Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. Gov. UK report.

## Measuring the underlying causes of behaviours

Measuring why behaviours are taking place is crucial when trying to change them. Failing to do so dents the chances of campaigns working.

How do you measure the underlying causes of behaviours? One way is to employ behavioural science frameworks like the **COM-B model**<sup>13</sup>. The model explains the influencers of human behaviours. Referring to the model can help you pinpoint the barriers to good security behaviour.

Based on a wealth of behavioural science research<sup>14</sup>, we know the following are important to measure:

Barriers	Description
 <b>Security frictions</b>	The extent to which security hinders productivity
 <b>Confidence</b>	A person's belief that they can tackle cyber threats
 <b>Risk perception</b>	How likely we think cyber threats are, and the severity of their consequences
 <b>Social influence</b>	The extent to which the actions of peers influence how your people behave
 <b>Sentiment</b>	A person's evaluation of all things relating to cyber security
 <b>Value alignment</b>	Whether cyber security aligns with our personal values and beliefs

13 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.

14 For a review of key factors influencing security behaviour, see ENISA (2019). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity and Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. Gov. UK report

## CybSafe's Meaningful Phishing Metrics

Most simulated attack tools teach staff how to recognise and report cyber threats. The tools usually record whether people:

- click suspicious links,
- disclose sensitive information,
- report suspected phishing emails.

That's a good start. But we also need to record why certain simulated attacks fool certain people. We can then address the root causes of insecure behaviours.

CybSafe metrics record **why** people fall for simulated attacks. For example, the metrics might show...

- That people within the **finance department**,
- are susceptible to **legal category** phishing emails,
- that use **authoritative language**,
- and **evoke panic**.

Armed with such detail, we can remind people that Legal will never ask for sensitive information via email, and will never induce panic or fear.

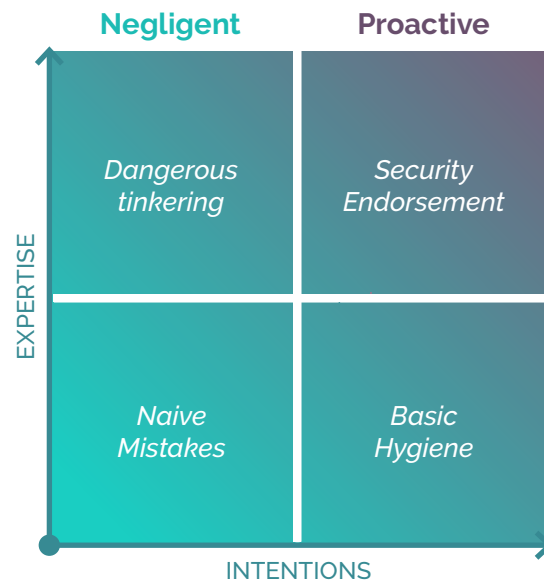


EXAMPLE



## Categories of security behaviours

Clearly, it's important to measure people's security behaviours. Security behaviours fall into four categories.



When measuring security behaviours<sup>15</sup>...

- **You should measure Naive Mistakes.** Naive Mistakes are unintentionally risky behaviours that do not require technical expertise. An example might be using a weak password.
- **You should measure Dangerous Tinkering.** Dangerous Tinkering behaviours are unintentionally risky behaviours that require some technical expertise. An example might be installing a browser addon that inadvertently allows outsider access.
- **You should measure Basic Hygiene.** Basic Hygiene refers to simple behaviours that mitigate cyber risk. An example might be installing routine software updates.
- **You should measure Security Endorsement behaviours.** These are behaviours that go beyond minimal security requirements. Think advocating security in the workplace!

When you know *what* people do and *why*, you can make your people a cyber defence.

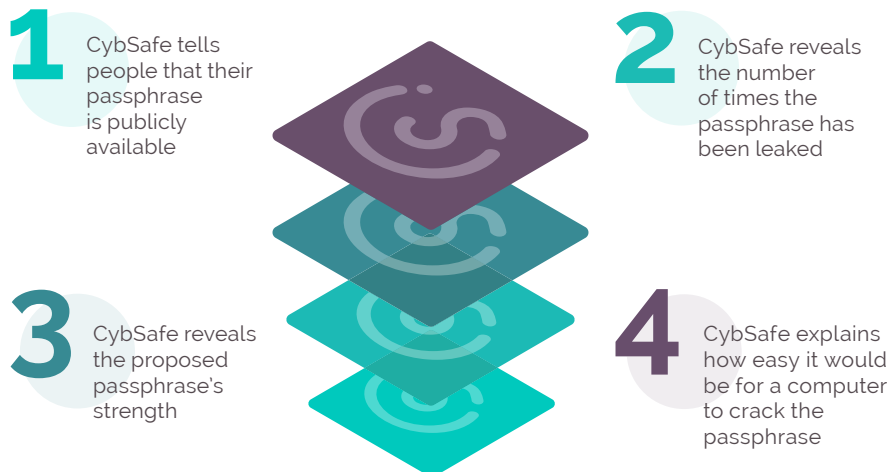
<sup>15</sup> Based on Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & security*, 24(2), 124-133.

 EXAMPLE

## Nudging people to change weak passphrases

Persuading people to use strong passphrases is tough. CybSafe uses the salience nudge to overcome the challenge. The nudge works by making information prominent. Here's an example.

On starting CybSafe, people are asked to set a passphrase. CybSafe checks all proposed passphrases to see if they've ever been breached. Whenever a match is found...



The four layers make the passphrase's flaws very prominent.

Finally, CybSafe recommends people change weak passphrases. People can skip the advice – allowing CybSafe to measure and improve intervention efficacy.

## Measuring Culture

Culture refers to a vision and set of values, shared by everyone in the organisation, that determine how people should think about security and incorporate security into the way they work. It is shaped both formally and informally by the organisation's physical and social environment and the wider society.

Organisations should assess their security (sub) culture along multiple dimensions that give insight into areas such as: leadership, employee perceptions, trust, employee understanding, resources, communication, behaviours enacted, environment etc. Organisations should be aware of areas where it is perceived that the security values and requirements conflict with the values and drivers of the individual (i.e. users may feel that security procedures prevent them from being productive).

Security culture influences cyber risk more than most imagine. People might know how to prevent threats. They might also value security. But they might take risks regardless – because that's the prevailing blueprint.

So advancing culture is important. It's also difficult. Culture is shaped by everything from corporate mission to floor plans. Plus, cultural "dimensions" are diverse. Leadership, employee perceptions, trust, resources, communication, behaviours; culture knows no boundaries. Subcultures add to the challenge of culture change.

Is the challenge insurmountable?

No.

And there are a few things you can do to make culture change possible.



## Start by measuring your existing security culture

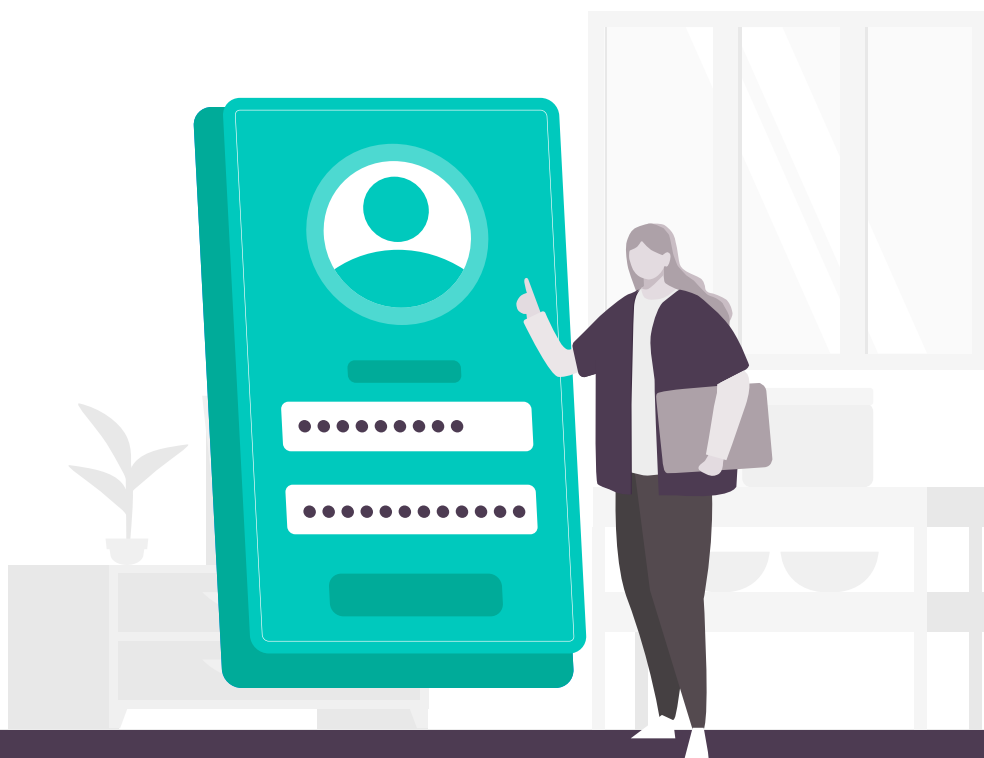
To start with, account for your existing culture. It's an essential step! Attempts to retrofit a new culture to an existing one almost always fail. A new culture is much more likely to take hold if it aligns with your current culture. So gauge your existing culture. Only then can you start to turn the right dials.

Of course, this highlights the importance of cultural metrics. The metrics should account for multiple cultural dimensions. Measuring culture at a granular level makes it possible to tease out the best course of action.

### EXAMPLE

#### The CybSafe Culture Assessment Tool

**C-CAT, the CybSafe Culture Assessment Tool**, measures security culture. The tool takes the form of a scientifically robust survey your people answer. C-CAT aggregates information on seven key dimensions. Each is scientifically proven to influence security culture.



## C-CAT Dimensions

 <b>Trust</b>	The confidence employees have in their organisation's cyber resilience.
 <b>Just &amp; Fair</b>	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.
 <b>Responsibility</b>	The extent to which employees view cyber security as being their responsibility.
 <b>Resources &amp; Communication</b>	The quality and quantity of cyber security communication material and training received at work.
 <b>Productive Security</b>	The extent to which employees feel they can be both secure and productive at work.
 <b>Ease &amp; Choice</b>	The levels of comfort and confidence employees' have when interacting with cyber security.
 <b>Community</b>	The perceived level of social acceptance towards security-related behaviours.

### EXAMPLE

As an example, consider the Resources & Communication dimension. You might think your people have access to everything they need to stay secure.

C-CAT shows people statements like "I know where to go to get information or advice about cyber security". Then it asks them the extent to which they agree. In doing so, it reveals insights into your culture. The tool even offers bespoke advice for building your security culture.

# Quality and Impact metrics

Getting to grips with your awareness, behaviours and culture metrics is a great start. Measuring ensures you're improving! But, the metrics are only part of the wider picture. As well as measuring each, you need to measure campaign quality and success. These tell us more about the performance of your campaigns.

## Quality metrics

In reality, security awareness, behaviour and culture (ABC) campaigns aren't always successful. What makes a campaign "succeed"? Or, for that matter, what makes a campaign "fail"?

What makes some campaigns better than others? Are there elements you should bake into campaigns for better results?

Quality metrics shine a light on ABC campaign performance. In doing so, they answer the above questions. Quality metrics help you refine and improve ABC campaigns. The metrics cover at least three areas:

- **Sources and modes of delivery**
- **Fidelity**
- **Engagement**



## Sources and modes of delivery

ABC campaigns come from various sources. Management can deliver campaigns, for example. But then so can IT teams, or security teams, and/or third parties. Delivery modes vary, too. Posters, e-learning, text messages, face-to-face training; ABC campaigns take many forms.

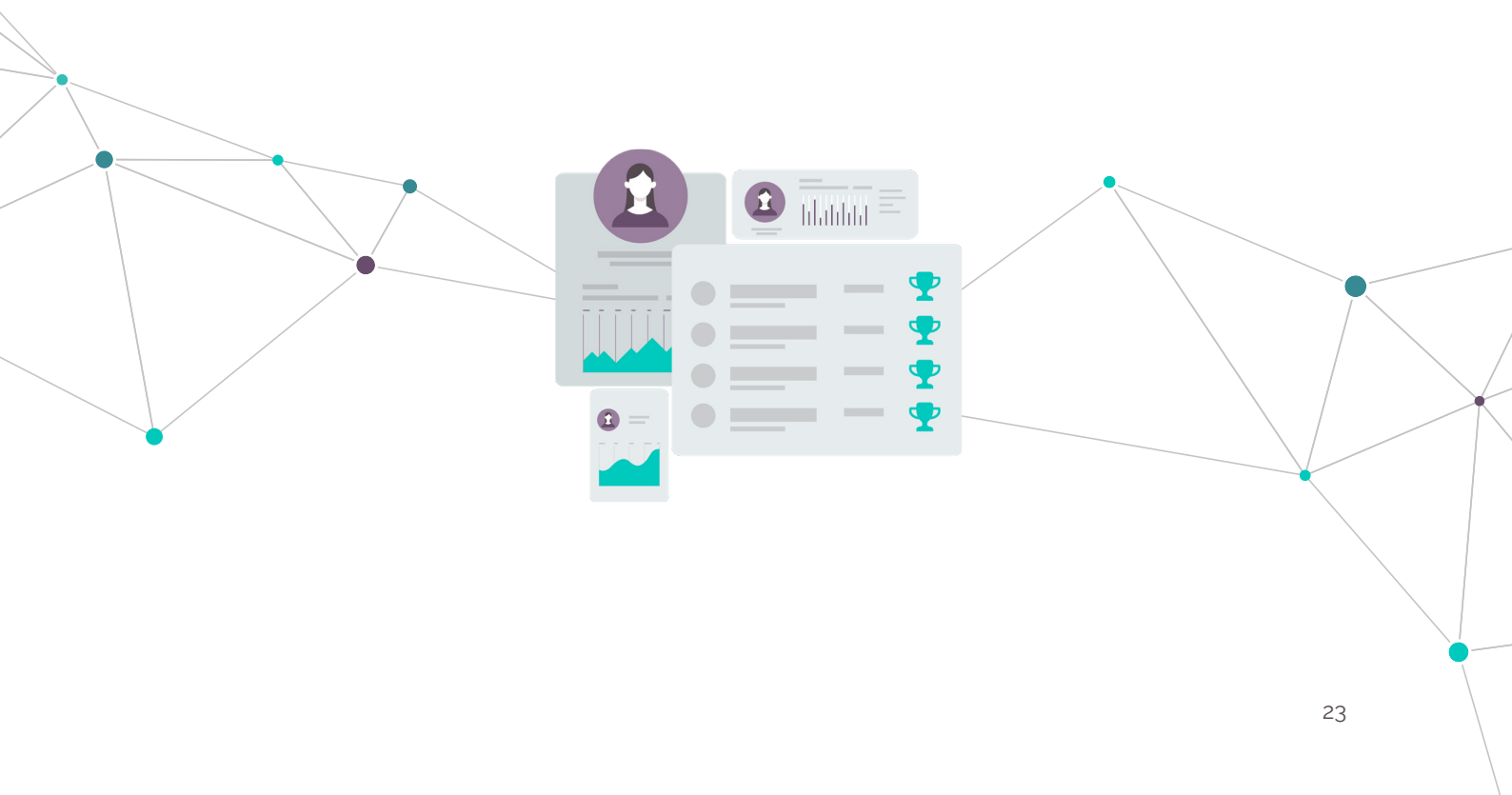
Recording ABC campaign sources and modes of delivery helps improve campaign performance.

## Fidelity

Fidelity assesses whether security campaigns were delivered as planned. Consider gathering metrics on the following:

- **Reach** - The extent to which an ABC campaign reached its target audience
- **Consistency** - The uniformity of a campaign across an audience
- **Practicality** - The extent to which barriers affected campaign success

Fidelity metrics help further improve ABC campaign performance.



## Engagement

Security engagement refers to two things. Campaign uptake is one; what people think and feel about the campaign is the other.

Research continually finds a positive association between campaign engagement and behaviour change<sup>16</sup>. That's what makes measuring engagement vital.

Security teams should use the following metrics to capture employee engagement with ABC campaigns:



### Duration

How long campaigns run for



### Frequency

How often people are exposed to campaigns



### Depth

The variety of content included



### Attention

The extent to which people process campaign content



### Interest

The feeling of wanting to know or learn more about security



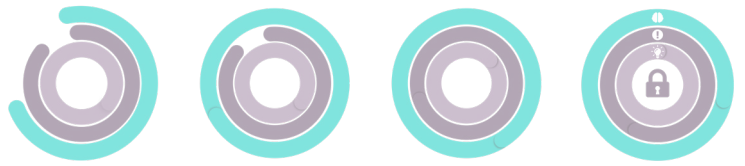
### Affect

Experiencing positive feelings and emotions

16 Perski, O., Blandford, A., West, R., & Michie, S. (2016). Conceptualising engagement with digital behaviour change interventions: a systematic review using principles from critical interpretive synthesis. *Translational behavioral medicine*, 7(2), 254-267.



# Impact metrics



Measuring success is challenging. But it's also necessary to reduce human cyber risk.

Impact metrics can help us answer the following about an ABC campaign:

- **Did it work?**
- **How well did it work?**
- **How did it work?**
- **What was delivered?**
- **Was it acceptable to those receiving/delivering it?**

Consider the following when evaluating impact:

- **What?** - What is your goal? Do you have one or many? If many, which is the primary goal?
- **When?** - When should measurements be taken? You should always measure before and after campaigns. Does continuous measurement also make sense?
- **Who?** - Who will measure outcomes? You? HR? Someone else? It's best to call on people with evaluation expertise.
- **How?** - How will the outcome be measured? How can it be verified? Training data? Computer logs? Interviews with staff?

## Impact metrics in a security reporting campaign

- **What?** - The primary aim of this campaign is to increase cyber security reporting of incidents.
- **When?** - First measurements should be taken before a new awareness communication. They should be updated quarterly.
- **Who?** - The security team will record measurements.
- **How?** - Outcomes and impact will be measured through the percentage of people that report a security incident pre, during and post campaign.



EXAMPLE

# Conclusions

Security interventions serve one key function: reducing cyber risk.

There are other functions. Providing ROI, for example. But reducing cyber risk sits above all else.

That seems simple enough. And yet working out which interventions reduce human cyber risk is difficult.

Most organisations try to do so in one way or another. But most fall back on shallow metrics.

Shallow metrics rarely reveal anything useful. They might show training uptake, for example. Or click-rates. Or report-rates.

But they're superficial metrics.

We need *meaningful* metrics.

We need metrics that cover security awareness, behaviour and culture. And we need metrics that help us check the performance of ABC campaigns.

By focussing on meaningful metrics, organisations can benchmark. We can assess progress. And we can measure with a view to reducing the risk inherent in the human aspect of cyber security.

Armed with meaningful metrics, we can reduce human cyber risk.



# ABOUT the AUTHORS



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

John is Head of Behavioural Science at CybSafe and a Chartered Psychologist with the British Psychological Society. He has a PhD in psychology and over eight years' experience in researching the connections between people and cyber security. John is passionate about helping people use technology in the most effective, safe and productive way they can.



**Joe Giddens**  
*Head of Content, Concepts & Community*

Joe is Head of Content, Concepts and Community at CybSafe. Joe is a former specialist detective in the Metropolitan Police Cybercrime Unit. Where he was responsible for the investigation, detection and prevention of complex online fraud and cybercrime. Joe enjoys taking complicated security ideas and making them simple.



**Oz Alashe MBE**  
*CEO & Founder*

Oz is a former Lieutenant Colonel in the British Army and UK Special Forces. His background gives him a unique insight into the socio-technical realities of cyber security and the sensitivities around changing human behaviour. Oz is the CEO and founder of CybSafe.

**CLICK HERE**

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