CYBSAFE // E-BOOK

How to use data to make your organisation more cyber secure

// CONTENTS

Introduction

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

Some measure security training. 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 best reduce risk?

Which provide the best ROI?

Meaningful metrics can help answer these questions. They can provide a benchmark against which to measure progress. They can help demonstrate success.

In this eBook, we'll explore how to measure security **Awareness**, **Behaviour** and **Culture**. Meaningfully.

Why is data important to cyber security?

Today, 42% of CISOs believe their boards do not fully understand the value and needs of the cyber security team.

Only 20% of boards are "highly confident" their cyber security team is effective.

> *We have to be able to quantify tangible impacts for boards – to quantify risk reduction, for example. Everything else is too abstract.*
>
> Richard Watson | EY Asia-Pacific Cybersecurity Leader

When it comes to cyber security, a lack of time, understanding and resources make it difficult to report meaningfully. We tend to focus on simple metrics. But such metrics in isolation are poor predictors of human cyber risk.

Take measuring "security knowledge" as an example.

Companies invest in security awareness training because it improves "knowledge" and achieves compliance goals.

But does better security knowledge really 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.

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

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. These need to be "meaningful".

A "meaningful" metric:

- Is appropriate for its security goal. For example, (1) password strength and (2) exposure in data breaches are good measurements of password hygiene.
- Is easy to interpret, understand, explain and act on.
- Is benchmarked. For example, against the industry average.
- Is reliable. Data checks should lead to the same result.

By contrast, a "bad" metric is difficult to understand. Bad metrics don't help with goal-setting. Nor do they aid decision-making. Use the SMART criteria to help you choose effective metrics:

- **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 tend to rely on measurements that provide numbers. But it's important to also consider measurements and insights that can't be counted.

Qualitative insights, such as interviews, focus groups and open-text employee feedback, are valuable. These types of insight provide 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. These give context to what you are measuring.

Knowledge alone is not enough

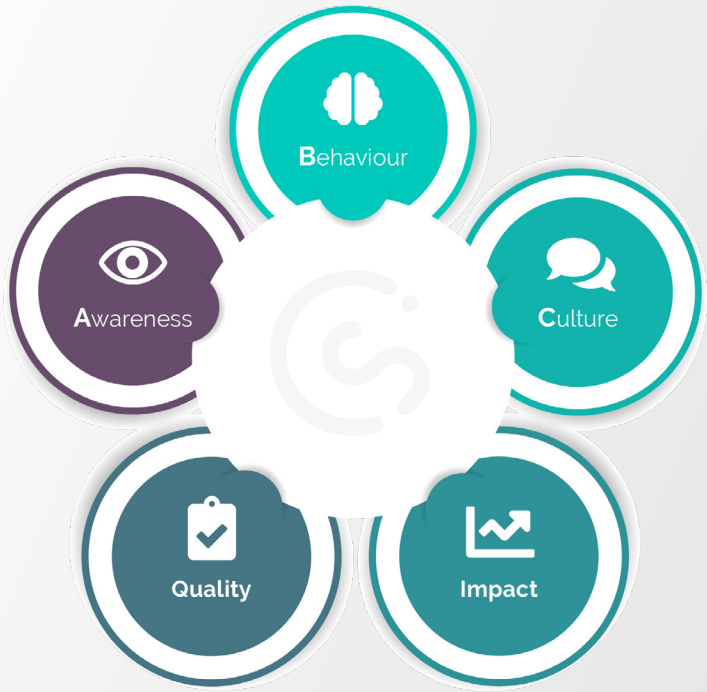
Most cyber security campaigns focus only on improving security awareness. This isn't enough. Better awareness rarely changes behaviour or culture.

Often people think "it won't happen to me." They may be aware their behaviour is insecure, but they'll carry on regardless. This leaves your human cyber risk unchanged.

Improving security awareness, behaviour and culture all at once is a much better ploy. Improve all three together and you reduce your human cyber risk.

Let's discuss measuring security Awareness, Behaviours and Culture (ABC) before we talk about measuring the success of ABC campaigns.

There are five metrics you need to measure:



Data that matters for human cyber risk

Measuring Awareness

Awareness refers to people's knowledge and understanding of cyber security risks.

Awareness interventions, which comprise education, training, support, and assistance, focus on making sure people know:

- **WHY** security is important for them personally and their organisation.
- **WHAT** they need to do to be safe.
- **HOW** to carry out security behaviours to reduce risk.

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

For certain, these metrics show the efficacy of people's short-term memory. Do they tell you much more? It's impossible to say.

When it comes to awareness, the strongest metrics focus on 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"

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

CybSafe's Awareness Metrics

EXAMPLE

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

- 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. Standardisation keeps metrics reliable across individuals and time.

Measuring Behaviour

Security behaviours include all direct and indirect actions that influence cyber risk.

Understanding why behaviours happen (or don't happen) allows facilitators and barriers to behaviours to be identified.

Barriers prevent or make it difficult to enact security behaviours. These include internal factors (such as mood, attitude and habit) and external factors (like workload and time pressure).

When it comes to behavioural metrics, focus on:

1. The behaviours you're **hoping to change** or promote.

2. And – the part that's most often neglected – **why behaviours are or are not happening** in the first place!

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.

The following influencers of human behaviour are important to measure:

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

CybSafe's Meaningful Phishing Metrics

EXAMPLE

Most simulated attack tools teach people how to recognise and report phishing emails. 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 these behaviours.

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

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

Armed with such detail, people can be reminded that Legal will never ask for sensitive information via email, and will never try to induce panic or fear.

Measuring security behaviours

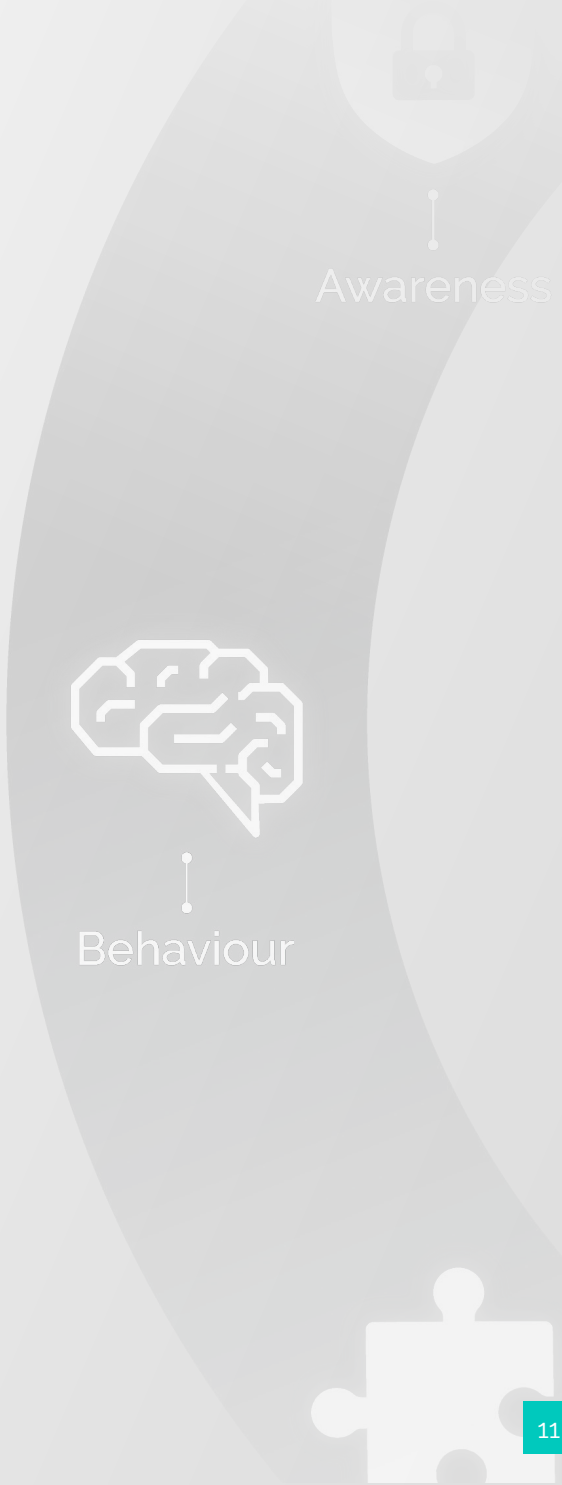
So, it is possible to measure why people behave as they do. But what about measuring security behaviours more generally across your organisation?

Behaviour-IQ is CybSafe's tool for measuring and tracking security behaviours.

You choose which behaviours to measure and track. Your organisation's existing data sources feed into Behaviour-IQ. You then receive a risk report from CybSafe. It contains appropriate interventions and recommendations to reduce human cyber risk.

This tool allows your organisation to understand and predict risk events caused by people.

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



Measuring Culture

Culture refers to the vision and set of values that determine how people think about security. It's shaped both formally and informally by the organisation's professional and social environment and by wider society.

Assessing security culture can give insight into the following areas:

- Leadership
- Trust
- Resources
- Communication
- Employee perceptions and understanding
- Behaviours
- Environment

Organisations should be aware of areas where security values and requirements are perceived to clash with the values and drivers of the individual. For example, people may feel security procedures reduce their productivity.

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 what everyone else does".

So, advancing culture is important. It's also difficult. Culture is shaped by everything from company mission to colleagues. Subcultures also 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.

To gauge your existing culture, you need cultural metrics. These metrics should account for multiple cultural dimensions. Measuring culture at a granular level makes it possible to tease out the best course of action.

The CybSafe Culture Assessment Tool

EXAMPLE

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

Trust	Employees' confidence in their organisation's cyber resilience.
Just & Fair	How fairly treated employees feel with regards to cyber security and how comfortable they are 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.
Ease & Choice Sentiment	Employees' levels of comfort and confidence when interacting with cyber security.
Community	The perceived level of social acceptance towards security-related behaviours

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.

Measuring quality and impact

Getting to grips with awareness, behaviours and culture metrics is a great start. Measuring makes sure you're improving!

These metrics are only part of the big picture. As well as measuring each, you need to measure campaign quality and success. These tell us more about the performance of 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"?

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.

Fidelity

Fidelity assesses whether security campaigns were delivered as planned. Consider gathering 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

Frequency

How often people are exposed to campaigns

Engagement

Security engagement refers to two things:

- Campaign uptake
- What people think and feel about the campaign

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

The following metrics are great ways to measure employee engagement with ABC 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

Duration

How long campaigns run for

Impact metrics

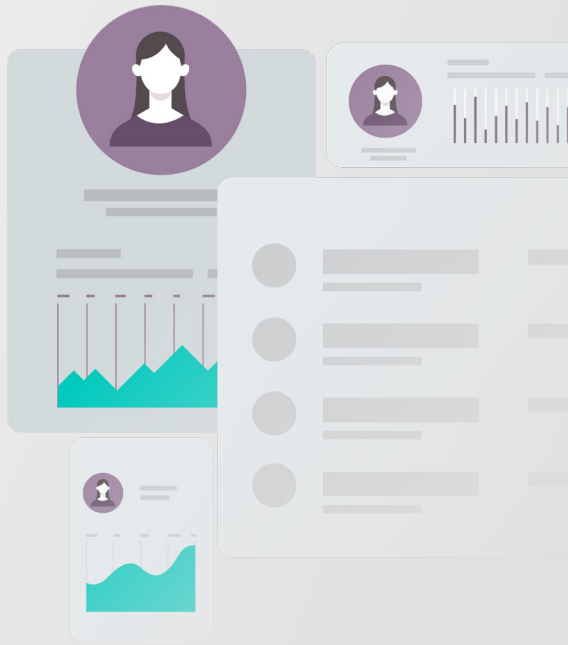
Measuring success is challenging. It's also necessary to reduce human cyber risk.

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

- **What was delivered?**
- **Did it work?**
- **How well did it work?**
- **How did it work?**
- **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.
  But continuous measurement can also be useful.
- **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?



Conclusions

Security interventions serve one key function: reducing cyber risk.

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

That seems simple enough. Yet working out which interventions reduce most human cyber risk is difficult.

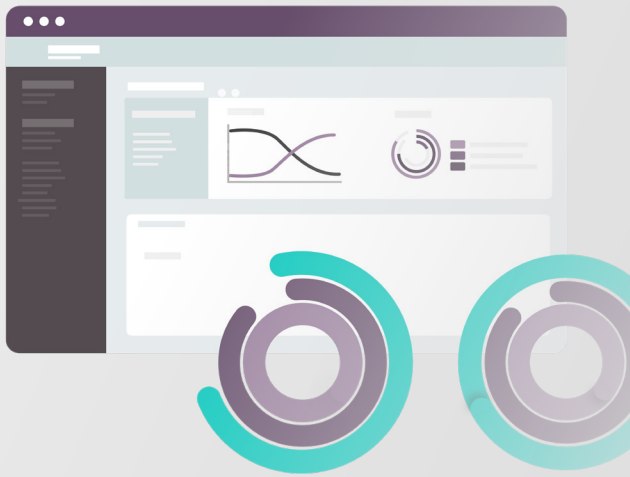
Shallow metrics rarely reveal anything useful. They might show training uptake, for example. Or click-rates. Or report-rates. But they're superficial metrics.

We need meaningful metrics.

We need metrics that cover security awareness, behaviour and culture. And we need metrics that prove the success of ABC activities.

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

Armed with meaningful metrics, organisations can demonstrably reduce human cyber risk.



Understand people. Prevent security incidents.

Contact us

To learn more about what we do, or to take a tour of the platform, just get in touch!

hello@cybsafe.com

0203 909 6913

Level39
One Canada Square
Canary Wharf
London E14 5AB