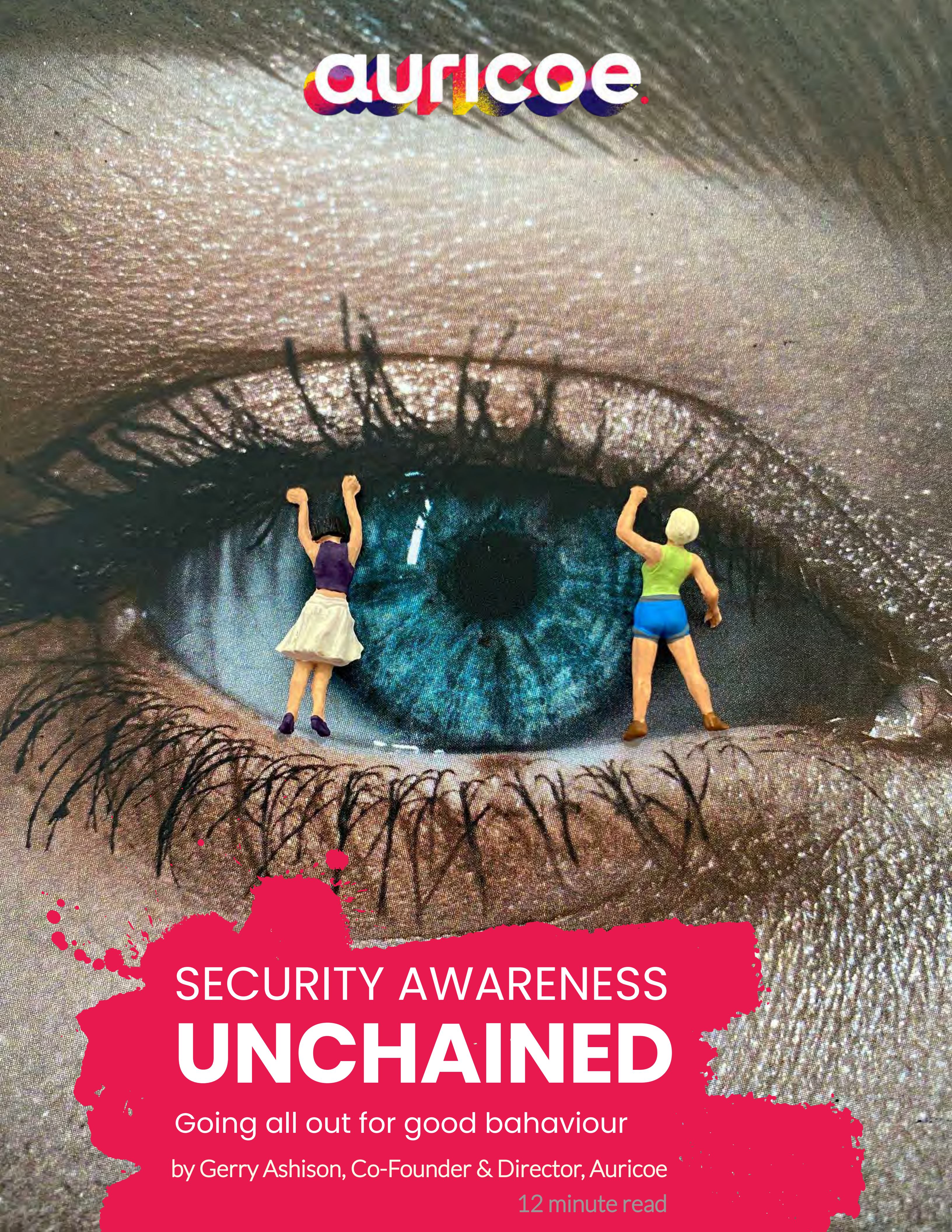


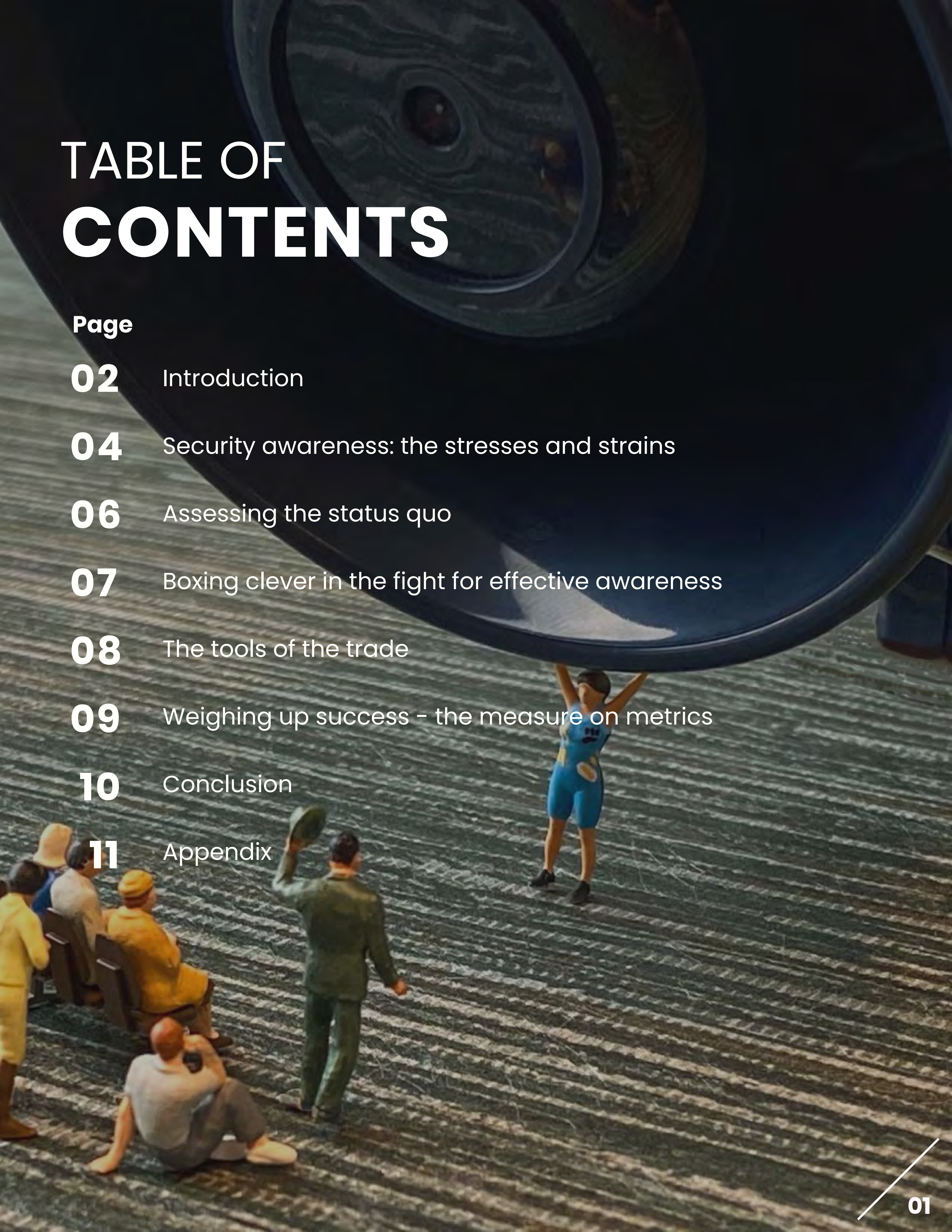
auricoe

# SECURITY AWARENESS UNCHAINED

## Going all out for good bahaviour

by Gerry Ashison, Co-Founder & Director, Auricoe

12 minute read



# TABLE OF **CONTENTS**

Page

# Introduction

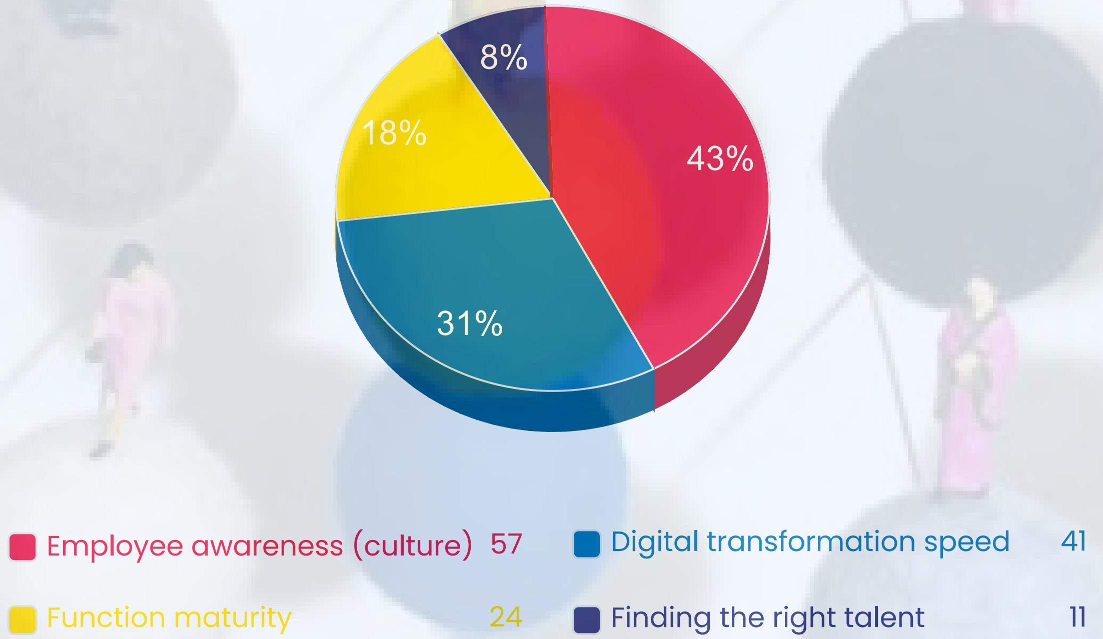
The human lungs are a fascinating organ. They boast the combined surface area of a tennis court and process over 9,000 litres of air per day, toiling to expel carbon dioxide and enrich our blood with oxygen – they work tirelessly to keep us alive.

They don't get to enjoy every weekend off; we don't always look after them as best we should, and their endeavours only tend to be pondered when under attack. A plight that I suspect many security professionals will empathise with - especially those of an awareness persuasion.

At the turn of the year, we polled opinion on the biggest challenges facing security functions over the prevailing year. Employee awareness finished head and shoulders above the rest - speed of digital transformation, function maturity, and the quest for talent completed the quartet. It makes sense when you factor the average cost of a data breach was c. £2.8mn as of 2020 (1), not to mention the vulnerabilities manifested by home working – the surface area for cyber-attack has our lungs turning green with envy.

## What represents the biggest challenge to security departments over the coming year?

LinkedIn Poll 15th January 2021 Total votes 133



Awareness, technology and governance form the backbone of loss prevention, but they do so from the wings. When the revenue-exploding stars work their magic, profits dazzle - products, services, subscriptions and advertising all offer stellar returns on investment. On the contrary, the very best that rules, tools, and the changing of habits can hope for is nothing lost and reputation gained - an old football adage springs to mind. Strikers win matches; defenders win leagues.

> **“ strikers win matches; defenders win leagues**

The parody of awareness-success being zero is confounded when determining the cost of a potential security breach. Health and safety failings result in injury or death. Hence the need to invest in this breed of awareness is incontestable. By comparison, we only ever know the extent of technology and security failings in their aftermath – sadly, swelling the security awareness budget, and channelling more time towards reducing human risk, requires somewhat more persuasion.

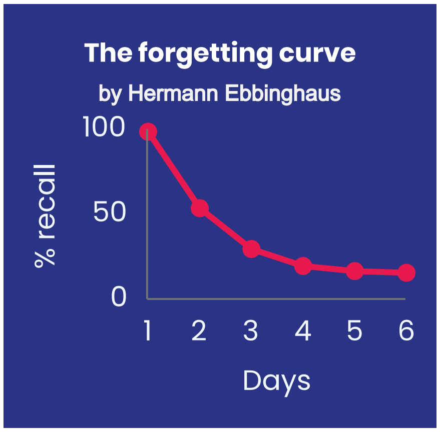
In this report, we examine the challenges that confront security awareness. We'll explore how to assess existing efforts and the individual components at an awareness professional's disposal. We then take a recce on metrics as a means of measuring and demonstrating awareness success.

LOCTITE
SUPER GLUE
Cyanoacrylate.
Danger. Bonds skin and eyes in seconds.
Keep out of the reach of children.
3g

# Security awareness; the stresses and strains

### Awareness by definition

Training and awareness are words that people use interchangeably, yet they are two very distinct disciplines. Training teaches us to take known variables, apply them to a given situation and achieve an expected outcome. Awareness, on the other hand, reshapes our cultural sensitivity to a topic. It enables us to react in a measured way to unpredictable events – situations that we haven't come across before. Short of psychic capability, the power of training is limited in thwarting the next cyber-attack. Changing our behaviours so that we show competency in the face of future threats is paramount.

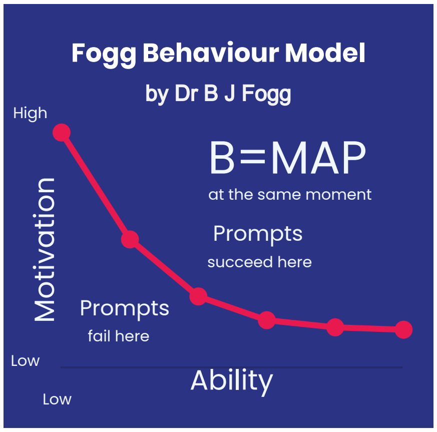


### The forgetting curve (2)

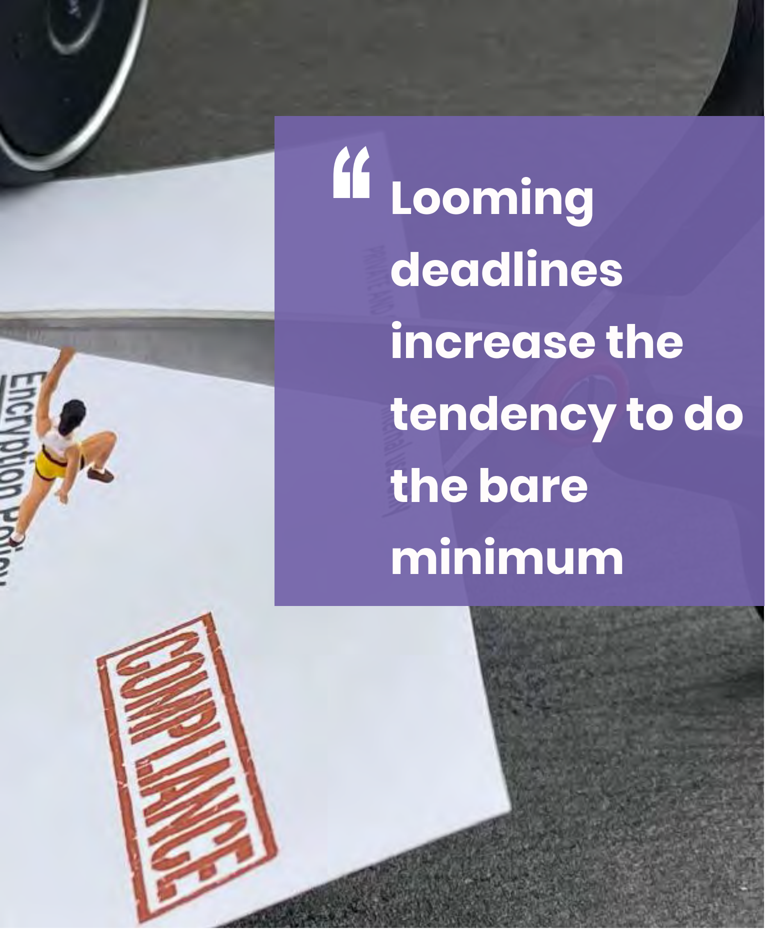
In 1885 German psychologist Hermann Ebbinghaus published his career-defining body of work - Memory. A Contribution to Experimental Psychology. A colourful cluster of experiments that founded the forgetting curve – illustrating our ability to retain information over time. This curve depends on subject complexity, information delivery, stress, sleep and other psychological factors. Repetition, memory techniques and level of interest can interrupt the curve - the perennial challenge for any awareness program.

### The Fogg Behaviour Model (FBM) (3)

Dr BJ Fogg founded the Behaviour Design Lab at Stanford University, creating models and methods in behaviour design. The FBM is a graph that plots a similar shape to that of the forgetting curve. This model highlights the need for a trio of elements - Motivation, Ability and a Prompt - to trigger behaviour. He posits that if any of the three is missing at that given moment, behavioural change does not occur.



> awareness reshapes our cultural sensitivity to a topic



> “Looming deadlines increase the tendency to do the bare minimum

### Compliance budget

The compliance budget offsets the need to toe the line against the work commitments of each user. When staff feel pressured by issues and looming deadlines, there is a tendency to do the bare minimum – even to cut corners on compliance. Each employee has a limit on the daily amount of time assigned to meeting compliance standards. As we cross that threshold, the cost of fighting for users' attention and getting them to do the right thing skyrockets. Increased monitoring, sanctions, stress and a lack of goodwill from users can inflict pain on an organisation's balance sheet. For awareness to change behaviour, efforts must focus on areas that matter most. We can also attempt to alter user perception of where this threshold should lie. (4)

### Ought to versus must do

Language is everything. If parking fines were optional, would you pay? Do the ICO issue non-compulsory penalties for data breaches? When loss mitigation is non-negotiable and becomes part of our job description – assessed in the same way as any other KPI – it alters our compliance budget threshold. We do what wouldn't otherwise get done.

### The blame game

Human error is responsible for 23% of data breaches. (5) Users need to show accountability. If all measures are in place – suitable tools, clear policies and a well-oiled awareness programme, we must hold employees to account. But this is a big 'if'. Users may be apathetic, overwhelmed, malicious or prone to a mistake; we should consider this before apportioning blame.

> “Users need to show accountability

# Assessing the status quo

Security awareness programmes are an intricate business. Scoping out the current landscape is crucial if the end goal is to optimise existing efforts and build that human firewall. There are several questions worth asking, and while the list below is by no means exhaustive, it offers a sound basis for such analysis.

01 What is the incentive for your existing awareness programme (tick-box compliance, risk reduction, or best-in-class)?

02 Do management support awareness efforts? If yes, how was this achieved?

03 Which awareness topics are you touting (phishing, malware, password security, removable media, safe-surfing, social engineering, physical access, clean desk policy, data management, use of personal devices)?

04 Which tools are you deploying (security champions, phishing simulations, computer-based training, newsletters, special events, meetings, posters, screensavers, marketing collateral)?

05 What percentage of efforts are off the shelf versus bespoke?

06 Does each awareness message carry sufficient impetus to act?

07 How often are you communicating and reinforcing your messages?

08 Which metrics are you using to track endeavours and outcomes?

09 Have you assessed how and why methods were effective?

10 Is the approach multi-faceted, targeting differing personalities, user groups and sub-cultures?

11 Does negligence lead to repercussions, and are compliance guidelines communicated clearly?

# Boxing clever in the fight for effective awareness

> “ Security awareness is behind the curve when compared to HR L & D and could gain a lot by drawing from that discipline and talent. *Sumita Hodgson, Security Awareness Lead, Aveva*

## Check out the competition

It's always worth taking a peek at the competition. Indeed, your wider industry as a whole. Understanding what's gone before can serve as a powerful lever and assist you once the focus shifts to looking inwards.

## The mood in camp

Culture is the beating heart of any awareness program – it drives the behaviour that awareness seeks to change. Understanding your organisation's overall culture is paramount, but that isn't where the story ends.

Geographic spread, disparate entities, a variety of functions and diverse approaches all lead to distinct subcultures.

Are users communicating via mobile or desktop? Are employees field-based, and do they meet regularly? Are there figureheads with influence? Effective awareness must cater for all.

## Relationships are your biggest ally

Users hold a wealth of knowledge - not least, why they do what they do, what goes on within the organisation, and what does and doesn't work. They will also be aware of previous programmes and offer priceless suggestions for future efforts.

## Pillars of support

One expects a certain synergy between technology, security and awareness teams, but awareness professionals must pool additional resources elsewhere.

Corporate communications can advise on standards, requirements, limitations, turnaround time, and so much more. Legal and compliance impart policies, procedures and a governance framework, alongside essential sanctions when actions fall short.

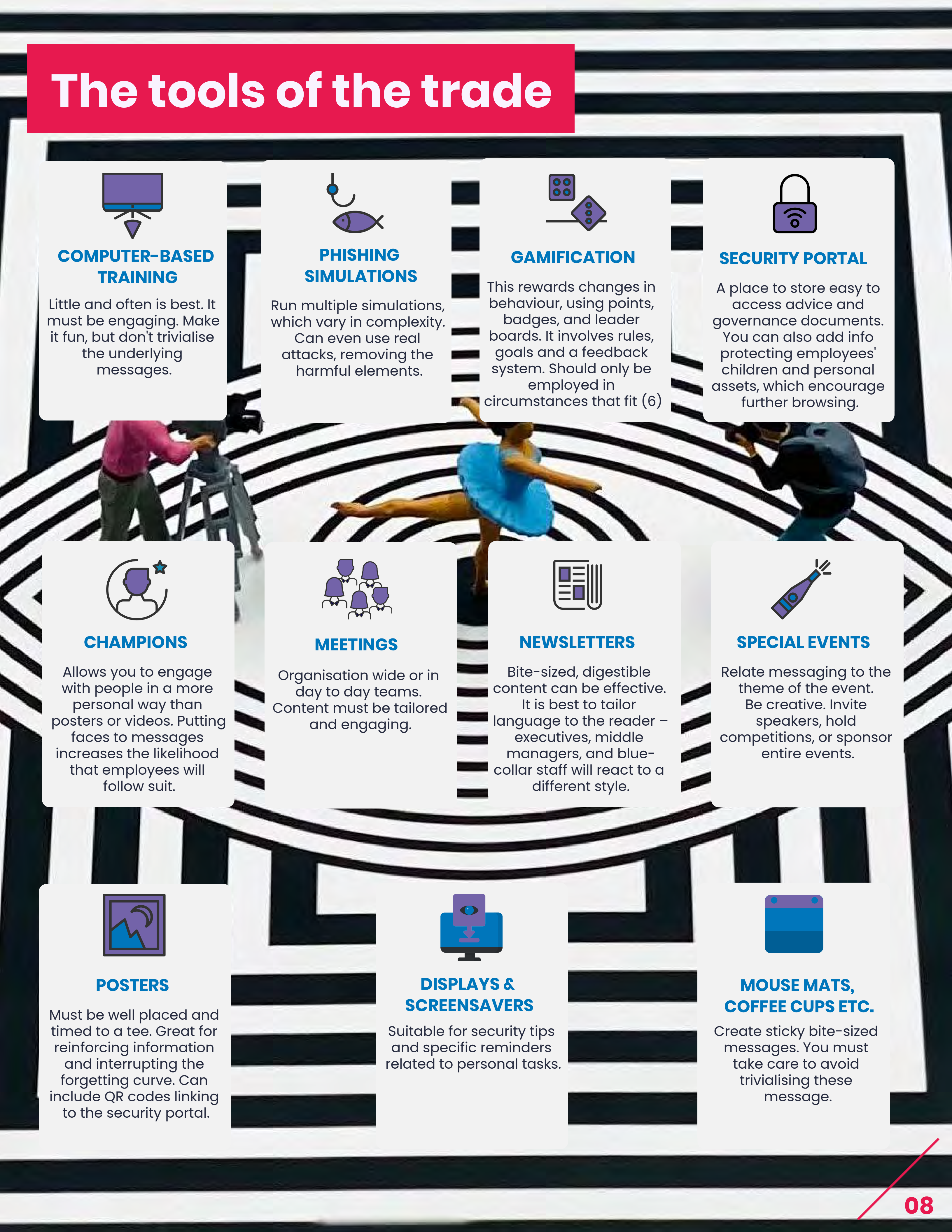
Human Resources are often the guardians of company culture, shedding light on the organisation's inner workings.

"The HR Learning & Development function is very human-centric and draws a lot from behavioural psychology, which fits well with what security awareness strives to achieve. There is also a well-established framework of measurement. Security awareness is behind the curve when compared to HR L & D and could gain a lot by drawing from that discipline and talent." says Sumita Hodgson, Security Awareness Lead, at Aveva.

Then comes physical security, assisting with distributing materials, collecting metrics, and knowing facilities, which can all prove invaluable.

Last but by no means least, there is Health and Safety. A department with the inside track on successful outreach methods. They are also familiar with operating under the microscope. Sharing security awareness messaging across their well-trodden communication paths can lighten your load and add weight to your efforts.

# The tools of the trade



### COMPUTER-BASED TRAINING

Little and often is best. It must be engaging. Make it fun, but don't trivialise the underlying messages.

### PHISHING SIMULATIONS

Run multiple simulations, which vary in complexity. Can even use real attacks, removing the harmful elements.

### GAMIFICATION

This rewards changes in behaviour, using points, badges, and leader boards. It involves rules, goals and a feedback system. Should only be employed in circumstances that fit (6)

### SECURITY PORTAL

A place to store easy to access advice and governance documents. You can also add info protecting employees' children and personal assets, which encourage further browsing.

### CHAMPIONS

Allows you to engage with people in a more personal way than posters or videos. Putting faces to messages increases the likelihood that employees will follow suit.

### MEETINGS

Organisation wide or in day to day teams. Content must be tailored and engaging.

### NEWSLETTERS

Bite-sized, digestible content can be effective. It is best to tailor language to the reader – executives, middle managers, and blue-collar staff will react to a different style.

### SPECIAL EVENTS

Relate messaging to the theme of the event. Be creative. Invite speakers, hold competitions, or sponsor entire events.

### POSTERS

Must be well placed and timed to a tee. Great for reinforcing information and interrupting the forgetting curve. Can include QR codes linking to the security portal.

### DISPLAYS & SCREENSAVERS

Suitable for security tips and specific reminders related to personal tasks.

### MOUSE MATS, COFFEE CUPS ETC.

Create sticky bite-sized messages. You must take care to avoid trivialising these message.

# Weighing up success

## THE MEASURE ON METRICS

Awareness and HR professionals share striking similarities. Both offer services to employees and are culture-centric. Their shared purpose is to protect their organisation, but they also display unavoidable differences. HR is a distinct department, existing in every company above a specific size and containing staff that perform clearly defined roles. You cannot say the same for awareness. They limit losses rather than increasing profit, offering intangible benefits that never grace the balance sheet. Gartner tells customers that as of 2019, 60% of organisations just want to "check the box." (7)

The truth is that without shouting out, calls for increased awareness budget often go unheard. We must force unseen benefits into the spotlight. Cue metrics.

### DAY ZERO

It is impossible to show how far you've come without knowing where you started. The time invested will pay dividends down the line, bolstering the business case for additional investment.

### COMPLIANCE METRICS

Demonstrating adherence to compliance regulations and requirements is relatively straightforward and can be easily tracked, monitoring warnings, fines and worse. The potential for being shut down or even personal prosecution makes the justification for this particular breed of metric straightforward.

### ENGAGEMENT METRICS

These fall into two categories - attendance and likeability metrics. Attendance relays voluntary turn out to events and can also measure the accessing of information in your security portal. Likeability metrics rate training, events, meetings and gamification, usually on a scale of 1 to 5. Likeability doesn't always equate to understanding, knowledge retention or behavioural change, but it does increase the chances of all three occurring.

### BEHAVIOURAL IMPROVEMENT

Gathering these metrics is not an exact science and can be costly. Tracking incidents such as downtime, malware attacks, successful phishing attempts, lost USB drives, data compromises, and more is an excellent way to measure altering behaviour. Gamification can also be highly effective when done well and used in the right circumstances.

### TANGIBLE ROI

Assigning monetary value to loss reduction efforts is a tricky business. Depending on industry and type of organisation, putting in the research miles can uncover highly relevant information about the costs of user-initiated loss. There are companies out there that have invested heavily in gathering actuarial data to support monetary worth.

### INTANGIBLE BENEFITS

Here we must hark back to relationships. Talking to users, stakeholders, and other awareness professionals can bring further gains to the fore. The intangible benefits to an organisation may outweigh the tangible.

# Conclusion

According to Verizon's 2020 Data Breach Investigations Report (DBIR), user errors are now as common as social breaches, and only hacking remains more prevalent (8). Apathetic and overwhelmed users pile on the misery, highlighting the worst-kept secret in security – awareness efforts need improvement.

**Useful suggestions**

**Demonstrate value at every turn**

Measuring is as vital as messaging.

**Where there's a will, there's a way**

Research stakeholders, try to grasp personal interests and assess whether awareness efforts can address individual needs.

**Talk on their terms**

Use language that resonates with your stakeholders and highlights support for strategic objectives.

**Spice it up**

Captivate users and interrupt the forgetting curve as often as humanly possible – without overload. Rotate messages and their means of delivery to keep users engaged.

**Have no fear of perfection; you'll never reach it – Salvador Dali**

The aim is to communicate how to perform tasks safely and make better judgements.

**Bespoke is best**

Tailor efforts to the individuals and siloes that power your organisation.

**Where reputation grows, money follows.**

**When organisations go to the ends of the earth to protect data, they enhance their standing and unearth opportunity.**

# Appendix

01 https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

02 https://onlinelibrary.wiley.com/doi/abs/10.1002/0470018860.s00657

03 https://behaviordesign.stanford.edu/fogg-behavior-model

04 The compliance budget: managing security behaviour in organisations Beautement, A., Sasse, A. & Wonham, M. (2008)

05 IBM Cost of a Data Breach Report 2020 - https://www.ibm.com/security/data-breach

06 The Gamification of Learning: a Meta-analysis Sailer, M. & Homner, L. (2020) https://link.springer.com/article/10.1007/s10648-019-09498-w

07 You CAN Stop Stupid - Winkler, Ira; Brown, Tracy Celaya.

08 IBM Cost of a Data Breach Report 2020 - https://www.ibm.com/security/data-breach

For more info visit auricoe.com or email us on valued@auricoe.com