Protect • Comply • Thrive

5 Reasons Your Security Awareness Programme Isn't Working

Five reasons your cyber security awareness programme isn't working

With the continuing rise in cyber security threats, many organisations recognise the need to invest in a comprehensive cyber security awareness programme, but the success rate of these interventions rarely corresponds to stakeholders' expectations.

The reasons for this gap between stakeholder expectations and reality are diverse, and, perhaps surprisingly, not always budget related.

To gain a deeper insight into the problem, our team of cyber security and learning experts has examined the **five most common obstacles** that organisations of all sizes fail to overcome when developing a cyber security awareness programme.

1. The lack of a common purpose supporting the business objectives

Challenging timescales to comply with security standards or regulations often make organisations lose sight of the underlying business objectives that should drive their awareness programme.

When strong objectives such as 'cutting cost', 'gaining access to new customers' or 'reducing risk' are replaced by statements such as 'all employees need to take the training and pass the test in time for the audit', you know that your awareness programme is heading in the wrong direction.

This lack of clearly defined business objectives at the outset of a programme rapidly results in disengaged stakeholders who view it as a mere tick-box exercise, to be completed as quickly and as cheaply as possible. This leads to equally disengaged audiences that perceive the programme as a bothersome duty on top of their daily workload.

If both stakeholders and employees recognise the business benefits as the key driver for awareness, they are more likely to invest the necessary time and effort to achieve lasting results.

This focus should be maintained throughout the entire delivery cycle, making business objectives the cornerstone of your awareness programme, from the planning stage through to evaluation using more business-focused metrics, such as the occurrence of incidents, or the financial gains resulting from raised awareness.

2. Failure to motivate your audience

Although the essential role of motivation in adult learning and behaviour change is widely known, most organisations fail to exploit it as a tool for building awareness. This is a particularly sore point when it comes to cyber security, as the correct behaviours to adopt are often considered to hinder productivity, meaning that any existing motivation can quickly be damaged once participants realise the implications of compliance.

As mentioned, a clearly defined business purpose for the programme

can be a first step towards fostering motivation. However, most employees need more encouragement.

Common techniques to raise motivation include applying gamification and game mechanisms, which make use of behavioural motivators such as reward, competition or loss aversion. There are more complex, cognitive and emotional factors that play an essential role in your employees' dedication to the programme. These are often more difficult to pinpoint and need to be addressed through a needs analysis.

Ultimately, motivating your audience starts with understanding them. What makes your learners tick? Perhaps they are driven by rewards, such as a prize draw, or integrating the programme into their personal development plans, or maybe they seek a sense of community.

Whatever it is that motivates your workforce, you need to identify it before designing a successful awareness programme and exploit it right from the start.

3. A focus on knowledge, rather than behaviour

Research shows, time and again, that high levels of cyber security awareness are not equivalent to reduced levels of bad practice. In fact, awareness is just the beginning of a long journey to sustained behavioural change.

Nevertheless, the trend of concluding a cyber security awareness programme with a simple test of employees' acquired knowledge prevails across most sectors. If you measure success in test scores only, then the impact of your programme probably won't reach beyond the domain of knowledge.

Other common mistakes in this area include a lack of concrete instructions and actions. Learners may leave your awareness intervention with a better knowledge of cyber security, but this does not mean that they will automatically adopt the right behaviours and refrain from opening corrupt attachments and other bad practice.

To fill this gap between 'knowing' and 'doing', organisations need to give their workforce clear messages and instructions on behaviours to adopt. This may seem evident, but when under pressure to deliver your programme, it can be easy to overlook the most apparent drivers for success.

Moreover, many organisations' cyber security awareness programmes fail to provide their employees with a context to the learning and realistic examples to follow, which, again, widens the gap between knowledge and behaviour. In order to change their behaviour, individuals need to know how the content studied applies to them in their everyday roles.

4. Poor timing and delivery

Even the greatest awareness interventions don't work to their full potential if the programme is not planned and delivered well. Timing is a critical factor that organisations ignore all too often.

There may be an urgent need to train your workforce, but this does not

mean that the programme has to be 'pushed out'. Instead, consider a phased roll-out, allowing you to meet some immediate requirements first, and then refine any interventions to follow.

In the past, a rigid waterfall approach was the principal method used to develop digital learning and awareness assets.

Although this is a reliable strategy for delivering small 'ad hoc' courses, organisations are recognising the benefits of more agile-style approaches, in particular when it comes to developing complete awareness campaigns.

5. Few components and the restriction to one medium

From browsing the news on our smartphones to scanning posters in a train station on our morning commute, we are surrounded and influenced by a wide range of different media formats. Yet when it comes to developing an effective cyber security awareness programme, many organisations limit their campaign to a single channel.

You may feel that you have few options for delivery, with the obvious choices including a cost-effective e-learning solution deployed to a learning management system or a face-to-face, classroom-style training intervention, and possibly a 'blended' approach that incorporates elements of both.

When faced with this fundamental design question of their cyber security awareness campaign, few stakeholders consider all the options available to create the best architecture for their programme.

Learning and internal communications campaigns are, in many respects, similar to marketing and advertising campaigns, with the common goal of influencing your subjects' behaviour. This view can help organisations to understand the need for less traditional, more media-rich approaches to their cyber security awareness programme.

Would corporations such as Apple or Amazon limit their marketing strategies to delivery through a single channel or medium? No.

To maximise the visibility and impact of your programme, you need to think of it strategically and choose multiple components and channels of communication that will resonate with your audience.

With the increasing availability of user-generated content programmes and easily accessible media authoring tools, your options are wide ranging: from podcasts to social learning platforms, to video-led training, your possibilities are vast.

Exploit them.

- A **learning needs analysis** to identify awareness gaps and learning requirements.
- An effective **multi-component awareness campaign** tailored to your organisational needs and culture.
- Hands-on support to **customise the programme** from a specialist consultant.
- **Tools and resources** to suit your organisation's diverse needs and keep your audience engaged.
- **Evaluation measures** to provide you with a reliable audit trail of the success of the programme.
- A **total solution** that addresses behaviours, ideas and organisational culture and brings about a transformative result.

Contact us today to find out more:

www.itgovernance.co.uk/security-awareness-programme

Resources

Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Bada et al., Global Cyber Security Capacity Centre, University of Oxford.
Awareness is only the first step, *A framework for progressive engagement of staff in cyber security.* Hewlett Packard Enterprise, Business White Paper.
Tips for running a staff awareness campaign, *Lincolnshire County Council.*
www.infosecurity-magazine.com/news/bad-security-habits-persist-despite/