Secure Behaviour as the key to effective Security Awareness

Less than 1 percent of information security budgets are invested in people, yet 99% of attacks leverage human error to succeed. This means security awareness is more important than ever, but due to the immaturity of this niche, many programs are ineffective. This article discusses common pitfalls and concisely outlines a data-based approach to security awareness.

Goal

Due to compliance requirements and the influx of (spear)phishing attacks, Security Awareness is high on the to-do list of many Information Security Leaders. The starting point for those that embark on the journey is often security awareness training, but without careful planning and consideration, failure will be the outcome.

An often-made mistake is setting the wrong goal. Even though "awareness" is the name of the game, it shouldn't be the goal of an awareness program.

Case in point: according to Stanford University's Center on Philanthropy and Civil Society, "*abundant research shows that people who are simply given more information are unlikely to change their beliefs or behaviour*", and "*research suggests that not only do campaigns fall short and waste resources when they focus solely on raising awareness, but sometimes they can actually end up doing more harm than good.*"

> "Always start with the end in mind"
>
> Stephen Covey

The ultimate goal of any security (awareness) program is the reduction of (human) risk to an appropriate level. And it isn't knowledge or awareness that impacts risk. It's behaviour. Knowledge and awareness are "merely" prerequisites.

Setting secure behaviour as the end goal may seem trivial but is highly impactful. Because metrics are a direct derivative, doing so will enable measuring risk to the business instead of just compliance to the program. In other words, instead of measuring attendance, completion, pass and fail, measurements may include the impact of the program on: the number of reported, prevented and/or successful incidents due to human error; projects that have information security involvement and requirements; the percentage of properly classified documents; and many more.

Engagement

Another common obstacle to an effective security awareness program is a lack of engagement. Even though instructor-led classroom training is excellent for motivating people and getting the right message across, it's also resource-intensive and therefore not scalable. On the other end, online training is highly scalable, but not necessarily engaging out-of-the-box. This is especially true when the trainee does not consider training topics to be directly beneficial, which is often the case with information security.

Since it's impossible to make classroom training scale across large audiences without increasing expenses significantly, the question is: How do we make online training more relevant and engaging?

Assess

The first step is to analyse the target audience. Similar to university courses having entry requirements to ensure students' prior education corresponds with the curriculum, it's important to understand the security proficiency of the target audience. So, since the goal of our program is to create secure behaviour, the initial analysis should be aimed at identifying unwanted (i.e. risky) behaviours; who are demonstrating them; why they exist; and how they impact the organisation's activities.

The traditional way to approach a security assessment is to conduct a gap analysis leveraging a control set. However, even the most established frameworks currently lack the depth regarding people-centric security to support this approach.

The alternative is to leverage survey-based methods. This allows even large organisations to quickly and comprehensively perform assessments of security knowledge, awareness and behaviour. Importantly, these survey methods are grounded in the latest assessment science research and provide reliable outcomes that help understand the audience's overall susceptibility to cyberattacks.

If desired, the understanding of the target audience can be further improved by leveraging traditional assessment components, such as conducting desk research (e.g. prior incidents analysis) and interviews.

Educate

The results of the assessment provide a behavioural baseline of the target audience that will enable the creation of target metrics. This provides program management with a useful steering mechanism and aids security leadership in communicating value to the business.

Assessment outcomes can further be used to make data-based decisions regarding the content of the awareness training program. For example, grouping employees by their level of knowledge of specific topics allows for the creation of tailored training curriculums (per group) that address the underlying proficiency gaps. The same can be done for groups that display similar (unwanted) behaviour.

An element that cannot be omitted in the context of education is content delivery. When establishing curriculums, the following criteria should be considered:

- Gamification;
- Cross-platform portability;
- Aligning content with personal goals;
- Style and tone;
- Content surveys.

Simulate

As mentioned previously, education will improve overall awareness but its impact on behaviour is limited. A good way to leverage the increase of employee knowledge and awareness is to perform simulations. This will provide them with the opportunity to put learnings into practice and improve their skill-level, while the organisation gathers valuable data regarding user behaviour.

Since email phishing is currently the main attack vector for many organisations, phishing simulations should be a component of every security awareness program. As a matter of fact, by deploying an automated phishing simulation platform, organisations lower phishing email click rates by 89% in 1 year on average.

Social engineering, USB and voice phishing simulations also deserve consideration to help gather diversified data while further improving employee risk awareness.

Direct

After completing several iterations of security training, some residual (unwanted) behaviours may still remain. These can be addressed by using Behavioural Change Campaigns. These custom campaigns are designed to change unwanted behaviour by manipulating either of three elements: motivation, ability and prompt.

To illustrate: In public restrooms, most urinals have a strategically placed sticker of a bug which, according to sound science, men can't resist because of a deep-seated instinct to aim at targets. This shows how motivation (satisfaction), ability (placement) and prompt (target) work together to obtain desired behaviour.

A Behavioural Change Campaign ideally lasts from 6 to 8 weeks and is focused on a single unwanted behaviour that poses significant risk. Its two main success factors are team diversity and – again – data. The former ensures that as many different perspectives as possible are taken into account when designing the campaign. The latter facilitates monitoring to detect any course deviations at an early stage so the campaign team to act accordingly.

Sustain

Once the organisation has matured its approach to security awareness, long-term sustainability of the program should be ensured by integrating behavioural security objectives into strategic functions.

For example, HR and the business may integrate behavioural security objectives into job descriptions to ensure they become a criterium for performance management, promotion, bonusses or special assignments (e.g. M&A projects).

Ultimately, the objective is to consistently influence behaviour throughout the employee lifecycle, until secure behaviour become the norm.

The approach described in this document was designed by Behaav and named the Resilient Workforce Method. For inquiries please contact communications@behaav.com.