CPNI
Centre for the Protection of National Infrastructure

CPNI: HAS IT WORKED?

AN EVALUATION GUIDE FOR AN INTERNAL SECURITY BEHAVIOUR CAMPAIGN

DISCLAIMER

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product-endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential, and including but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using the information contained in this document or its references. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

INTRODUCTION

Your security behaviour campaign's been underway for a while, so now's the time to see how it's getting along.

A quick and easy way to evaluate your campaign's performance is to run a staff survey. There are different ways of doing this - this guidance outlines some suggestions.

Your survey could be a quick, five-minute questionnaire that assesses:

- What campaign materials have been seen
- What message employees took from them
- What impact the campaign had on employees' behaviour

The answers to the questions will help you to evaluate what impact the campaign has had. Remember, the wider and more diverse the sample, the better. So think about surveying the following:

- As many employees as possible
- Employees from a range of departments/teams
- A sample of different demographic groups (e.g. males and females, a range of age ranges etc.)

In addition to running a staff survey, try to use data from other sources to support your evaluation of the campaign. For example, data on changes in numbers of breaches taking place (e.g. pass wearing, clear desk policy, IT compliance) can indicate whether a campaign is improving staff security compliance. Changes in numbers of reports from staff about security concerns can provide useful data on whether staff are being more vigilant towards signs of unusual or suspicious behaviour.

Speak to your IT monitoring team, physical security team, and/or HR for further ideas on what additional data might be available to you.

DESIGNING YOUR SURVEY

When designing your survey, think about including the following:

Qualitative questions

- These are open questions that allow people to express what they think in their own words (e.g. what messages did you take away from the campaign?).

- They provide a rich source of information, but can be more time consuming to collect and are harder to analyse and draw comparisons from.

Quantitative questions

- These are closed questions that only allow answers that fit into the categories that have been decided in advance (e.g. 'yes' or 'no', 'male' or 'female' or the extent to which someone agrees with a statement using a five-point Likert scale from 'strongly agree' to 'strongly disagree').

- They provide data that is quick to obtain (usually ticking a box) and can be easily turned into percentages as every person is asked the same question. However, because the responses are fixed, there is less scope for a person to reflect their true feelings on a topic.

Questions that cover the following six areas:

1. Can they recall the campaign without being prompted?
2. Do they recognise the campaign materials when they're shown them?
3. Can they recall the key messages of the campaign?
4. Did they understand why the campaign was implemented?
5. How did they react to the campaign?
6. How have they changed their behaviour since seeing the campaign?

TIP!

Try conducting the survey when staff are entering the building in the morning. They are more likely to be receptive to being stopped then than when going to get their lunch or when leaving to go home.

EXAMPLE QUESTIONS TO INCLUDE IN YOUR SURVEY...

(You'll notice that some of these are quantitative, like the demographics questions, and some are qualitative, opinion-based questions)

DEMOGRAPHICS

- What is your job title?
- What is your age?
- In which department do you work?
- How long have you worked here?

TESTING THE WATER

- What do you think are the main security threats we face?
- Do you know what security procedures are in place to address these?

AWARENESS OF THE CAMPAIGN

- Have you noticed any security campaigns being run here?
- If so, what have you noticed?
- Which of these materials have you noticed?
  - Posters
  - Quizzes
  - Guidebooks
  - Intranet articles
  - Other media
- Which of these materials had the most impact on you?
- Were you aware of the issues before the campaign started?

WHAT DID THEY TAKE FROM THE CAMPAIGN?

- What do you think are the main messages of this campaign?
- At whom are they aimed?
- How do they make you feel?

HOW HAVE THEY CHANGED THEIR BEHAVIOUR?

- How has the campaign impacted on your security behaviour? (e.g. no impact; reinforced what I was doing already; positive impact on my security behaviour)
- What specific security behaviours has the campaign reinforced or have you started doing? Why?
- Why has the campaign not had an impact? What additional support would you need to have a positive change on your security behaviours?
- How important do you feel these behaviours are to your personal security?
- How important do you feel these behaviours are to the security of your organisation?
- How has the campaign changed your attitude towards security?

CONCLUSIONS ON THE CAMPAIGN

- Did you find this campaign useful?
- How often should we be running campaigns like this?
- How would you improve the campaign?
- What ideas do you have about how we can encourage staff to continue demonstrating these behaviours on an ongoing basis?
- Do you have any other comments about this campaign or in general about our organisational security?

TROUBLESHOOTING
WHAT IF I DON'T GET THE RESPONSE I WANTED?

1. What if a large amount of employees can't recall the campaign materials?

It probably means they haven't seen them. Perhaps you need to rethink how visible they are and how they've been distributed. If after doing this a large number of staff still don't recognise the materials, it may be that you need to produce more, and consider a more impactful launch.

2. What if employees don't 'get' the key messages?

Ask yourself: 'Are the messages of the campaign clear to someone who has never seen this before?' There may be an issue with how you've layered and structured the messaging, or it may have been lost within too much styling. Have you used all the available materials to their fullest potential?

3. What if employees don't understand what we're trying to achieve?

It could be that the balance needs to be shifted to being more educational. Perhaps revisit your materials and see if they can be adapted into something longer, more descriptive and which offers more explanation.

4. What if employees are actually alarmed by the campaign?

This is unlikely, however, should it be the case, it could be that the campaign is a little too 'in-your-face'. It may be worth replacing some of the harder messages with something softer.

AND FINALLY...

You will have a good idea of the measures of success that are specific to your organisation. Overall, however, if the net result is that employees are more aware of themselves and their colleagues acting in a security-conscious manner, then your campaign has done its job.

TOGETHER, WE'VE GOT IT COVERED.

CPNI
Centre for the Protection
of National Infrastructure