Running a staff vigilance campaign

CPNI
Centre for the Protection of National Infrastructure

Running a staff vigilance campaign

1 Introduction

About this guidance

How your employees behave is a key indicator of your organisation's attitude to security. Vigilant security behaviour – such as showing awareness of one's surroundings or engaging with strangers – will show any hostile individual watching that it's not just security guards and CCTV they need to worry about. Alert employees are just as likely to spot suspicious activity and report it.

In a time of varied threats from diverse perpetrators, it's important that staff understand the role they can play in keeping each other, visitors and their organisation safe.

This guide will first give you an understanding of what constitutes good and bad security behaviour; and then help you communicate this across your organisation. It gives you the tools to run a 'staff vigilance' campaign, including links to professionally-designed supporting materials.

CPNI has trialled the campaign framework outlined below across a variety of organisations – with positive results. The advice and recommendations contained in this guide are also informed by CPNI's specially-commissioned research into reconnaissance conducted by hostiles (individuals who want to disrupt your organisation or harm your people, assets or reputation).

Empowered by an effective campaign of this nature, your organisation will benefit from:

- Security-savvy staff
- Increased reporting
- An engaged workforce, capable of taking on board additional personal security advice.

1 Introduction

Staff vigilance: a powerful deterrent

The sheer range and scale of threats today means that we have to be more pro-active in our measures to reduce the vulnerability of our organisations, our people and our sites. This means ensuring that the people who work at your site support protective security through their behaviour. Getting your workforce to behave in a 'security savvy' way, to be vigilant and to report suspicious activity can multiply chances of detection – as well as deter those with hostile intent who may be watching. Employing your workforce as additional eyes and ears can be a massive enhancement of your existing protective security.

Our research has shown that hostiles undertake reconnaissance to obtain information vital for attack planning. An essential part of reconnaissance is visiting the potential target. During this phase hostiles will observe the people who work at the site. If they observe a workforce that pays attention to their surroundings and who are vigilant, hostiles will conclude everyone is watching, and the chances of them being detected is high – a very powerful deterrent. Conversely, staff not paying attention to their surroundings and not showing vigilance could encourage hostiles.

We recognise that different organisations face different types or levels of threat. You may simply wish to make all your staff more aware of the behaviours you expect around your site, how vital it is to be on the lookout and the importance of reporting suspicious activity immediately. Alternatively, there may be a particular threat which means your staff themselves could be a target, perhaps because of where they work. In which case, you may wish to run a vigilance campaign that has greater emphasis on personal security, and the measures staff should be taking to reduce the risk of being targeted. (For further information on this, see 'Including personal security advice in your campaign' in Annex B.)

This guidance will help you whatever level of awareness you're intending to raise in your organisation. It gives you the tools to empower staff and demonstrate to them that simply by being mindful of how they behave they can contribute to their organisation's safety.

Next, let's look at the principles that underpin all effective security behaviour change campaigns.

Friendly Hostile

"Vigilant staff are one of the most off-putting factors for someone up to no good; it makes them think they are being watched and that they're likely to be detected and intercepted."

TIP: Prime your guard force

When taking steps to improve staff vigilance, do not forget to ensure that your security guard force is similarly supported. If your employees do not feel that their efforts to be vigilant are being supported by their security colleagues, they are likely to quickly lose interest. For advice on how to assess, improve and maintain guard force motivation, read our guide 'Guard Force Motivation' (see Annex D).

2 Guiding principles for a successful staff vigilance campaign

2.1 Explaining the threat

Motivation is fundamental to behaviour change. Unless employees understand the threats they and their organisation face, they will not be inclined to change how they act. Educating staff about the nature of the threats, their potential impact and the role we can all play in countering them is therefore critical.

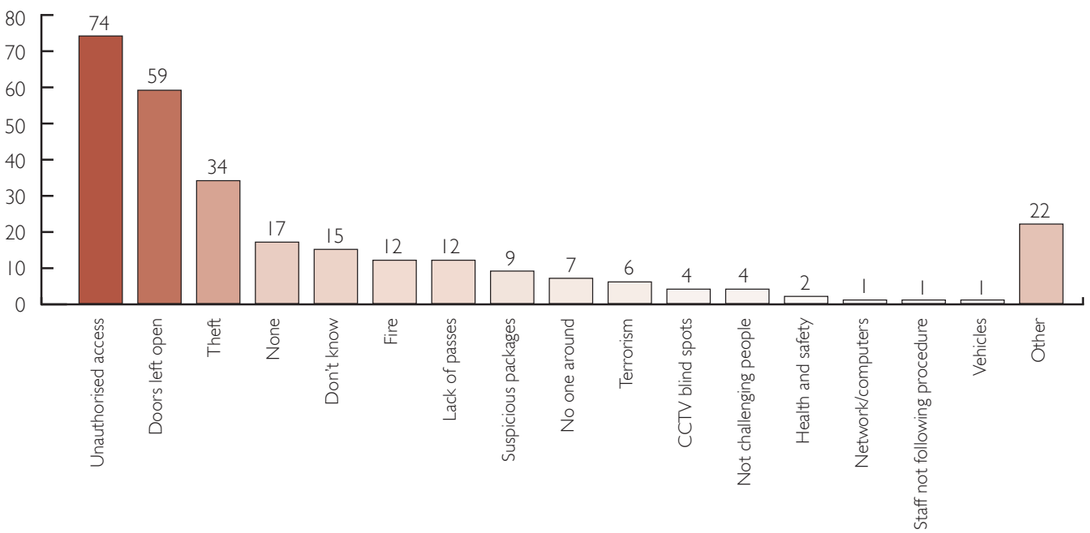
While threats will vary from organisation to organisation, what remains constant is the impact a vigilant and security-savvy workforce can have on deterring those who wish to do harm. Whether the threat is of a petty or more serious nature, a successful campaign will make staff aware of how cunning individuals could potentially try to harm them and their organisation and how staff behaviour can greatly assist, or conversely undermine, the protective security measures a site has in place.

2.2 Demonstrating the part staff play

There is a risk that staff can be complacent about threats and sometimes believe they have no contribution to make to their organisation's security. This complacency stems from a fundamental lack of awareness among staff of the risk they themselves can pose to security. Our research shows that when asked what they believe to be the main security risks facing their organisation, staff tend not to think of themselves or colleagues as the main risk. Instead they cite observable breaches in security.

Figure 1 – Unauthorised access is the most common risk cited by employees

When asked about the main security risks, staff cite factors around the manifestation of risk – e.g. unauthorised access and open doors



In this guidance, we will help you educate staff on the role people play in security – and how their behaviour can help to deter hostiles. Education, however, is just one part of a campaign to change security behaviours.

To embed security-savvy instincts, we will look at five 'E's in total:

- **Education**
- **Endorsement**
- **Ease**
- **Enforcement**
- **Evaluation**

Next, we'll elaborate on each of these 'E's, and what they mean in practice.

2 Guiding principles for a successful staff vigilance campaign

2.3 The five 'E's

The first 'E' is for Education

To educate staff, you need to communicate why their vigilant security behaviours matter and what is expected of them. We can therefore break 'education' into two component parts:

1. Education on the threat

Staff need to be aware first of all that the threat is real. It's important they understand that an incident could happen at any time, in any place and they – along with colleagues and the organisation as a whole – could be the target.

However, remember to counterbalance this necessary awareness of danger with reassurance about the measures you have in place to keep your people and your site safe. We tend to find that staff can be naïve about the type and extent of security measures in place. So explain how your control room works, the use of dog patrols and the quick response of security officers. Consider organising staff tours of your control room or meetings with security staff such as dog handlers.

TIP: Through the Hostile Lens

Ask a credible security expert (either from within or outside your organisation) to talk to your staff about the sheer variety of the threats out there. These could be from the small-time thief all the way through to the organised criminal, violent protester, terrorist groups or even state-sponsored espionage. Demonstrate to them the harm that such individuals and groups can potentially do to an organisation such as yours.

Educating staff about the threat, and what you have in place to help counter it, not only helps allay concerns but leads on to the idea that employees too have a role to play in security. There is only so much security can cover at a site at any one time; so we all have a part to play in helping to keep each other safe.

Think about how best to deliver these messages to staff. This could be via your intranet, newsletters, staff briefings etc. Ask staff how they prefer to receive communication from their organisation.

FURTHER READING: Threats come in many forms

As part of our 'Security-minded comms' guidance (see Resources section in Annex D), we have put together information on the different types of individuals and organisations that can seek to harm your staff, buildings and processes, and provided insight into how they think and operate.

TIP: Meet security

Consider running a security event or series of events for staff, where you can showcase the protective security measures you have in place. Ensure that those involved clearly communicate the key role that staff have in helping security protect their workplace.

2. Education about the part employees play

Take staff through the detailed planning process that hostiles go through to attack an organisation and create the realisation that they have the power to encourage or deter a hostile.

Outline for staff the sort of behaviours that would signal to a hostile that the organisation might be an easy target; we describe these as 'encouraging' factors. Some of these are listed below, but there may be factors that you can add from your own organisation's perspective. Conversely, outline for staff the sort of behaviours that would signal to a hostile that the organisation would be a difficult target; we describe these as 'discouraging' factors.

Hostiles will notice both manifest signs of vigilance, such as staff being obviously observant, and more subtle signs, such as content on your website that hints at the organisation having an observant workforce. (See our 'Security-minded comms' guidance for more about subtle deterrence messaging). Similarly, seeing internal vigilance posters in and around the building will serve to reinforce the perception that staff are vigilant at this organisation (see Annex E).

Behaviours that encourage hostiles	Behaviours that discourage hostiles
• Smoking just outside the building • Colleagues leaving together and generally not paying attention to their surroundings • Always taking the same route to work • Wearing headphones when entering/leaving the building • On a mobile phone outside the building	• Staff paying attention to their surroundings and being generally vigilant as they enter or leave buildings • Staff willing to engage where appropriate ("Can I help you?") • Visible posters which encourage staff vigilance • Vigilant Security staff who are quick and efficient when reacting to an incident
'Sloppy' personal security behaviours can make employees vulnerable by revealing a lot about their 'pattern of life'.	Vigilant staff are one of the most off-putting factors for someone up to no good; it makes them think they are being watched, and that they are likely to be detected and intercepted.

Definition: pattern of life

'Pattern of life' information is anything that provides details of a person's normal routine: where they live; their journey to work; facts about family and friends; where they socialise etc. Hostiles can use this information to gain someone's trust, disrupt their activities or even endanger them.

2 Guiding principles for a successful staff vigilance campaign

One organisation's experience: the 'friendly hostile'

"We asked a 'friendly' criminal to come in and help us 'think like the criminal'. He demonstrated that individuals up to no good do not hold all the cards and that it doesn't take a lot to put off even hardened criminals from their targets. For example, he explained that simple behaviours such as employees visibly showing awareness of their surroundings as they leave a building indicates that they are security-savvy and have a good security attitude. Such behaviours are deterring and can thwart attack planning."

TIP: "Can I help you?" A powerful deterrent at everyone's disposal

Our research shows that the prospect of staff engaging in a customer-friendly way is a strong deterrent for a hostile conducting reconnaissance. A simple "Can I help you?" conveys that staff are not only good at spotting people out of place but, critically, will do something about it by approaching them.

If you run an open site or one with frequent visitors, encourage staff to be customer friendly and helpful; if they see someone loitering or perhaps in a place they shouldn't be, they can enquire if they need help (before reporting in to security if they feel it was suspicious).

The second 'E' is for Endorsement

Having the right message, and medium to disseminate it, is only part of the story. You must decide who will be the 'voice' of your campaign. Who has the greatest credibility? Who will make the message really resonate with staff?

At work, we're bombarded with requests to 'do this' and to 'do that'. So a successful campaign relies on having significant others from inside the organisation (or outside where appropriate) to tell staff that their vigilance and reporting are important.

Different staff audiences might need endorsement from different people. For example, if you have a significant, cynical group of staff then you may consider that endorsement is best coming from a credible external expert. For new, keen staff attending their induction course, the message may be best delivered by the head of security.

Regardless, the message should be endorsed from the top – through written communications and staff announcements from the head of the organisation.

The security manager too has a key role to play in reinforcing the message and communicating that they are the 'go-to person' for any reports of suspicious activity (also see the 'Ease' section below). We have seen how the personal touch can help; for example, having the head of security quoted through internal communication channels saying just how much they valued a report-in from a staff member and what they did to action the report.

Think laterally about all the different occasions where the messages can be delivered and endorsed: for example, induction training, staff get-togethers and staff review meetings.

TIP: A timely reminder

Have security officers at your organisation hand out an aide memoire to staff (e.g. a leaflet, wallet card) as they arrive at work, to help reinforce messages around personal security and the need to look alert.

2 Guiding principles for a successful staff vigilance campaign

The third 'E' is for Ease

We have found that if you want staff to practise vigilant security behaviours you have to make them easy to adopt.

This means providing simple steps employees can take to improve personal security behaviours, and ensuring that they know what to look for and exactly how to report suspicious behaviours. Some key pointers for staff might include:

- **How to interrupt the 'pattern of life' impression you might be giving a hostile.**
- **How to give an appearance of vigilance.**
  For example, by enquiring "can I help you?" if someone appears out of place or is acting differently. This is especially important at open, crowded sites.
- **What to look out for.**
  A list of suspicious activities is really useful (our posters and supporting materials can help. See Annex D). For example:
  – Loitering around or near restricted areas
  – People taking photographs of staff or security features of the building
  – Someone taking an interest in staff/vehicle movements
  – Inappropriate approaches to any staff member
  – Someone being followed
  – Packages/bags being left unattended
  – Suspicious vehicle activity in close proximity to your site
  – Anything you feel isn't right
- **Exactly what to do if you do see something suspicious.**
  Make the instructions for reporting clear, and have them widely communicated throughout the organisation. For example, a button on the intranet homepage which takes you directly to the Security page and the control room number.
- **How to contact the security room and to locate your security officers.**
- **Emphasise that reporting will remain confidential and be taken seriously.**
  Employees should feel they are doing their job – not 'telling tales'.

TIP: Keep this number handy

Make the security control room number easily and widely available. Think about giving staff a wallet card featuring the number, which they can carry around with them when they are on and off site. See Annex D for an example wallet card.

The fourth 'E' is for Enforcement

This 'E' is all too often forgotten. Behaviour change cannot rely on education alone; staff are human and bad behaviours can all too easily become the norm. Without punitive measures for lapses or breaches in security, bad behaviours prevail. 'Deterrents' are fundamental to awareness and part of a multi-layered approach. The central premise is that staff will have a 'relaxed attitude' to their personal security if detection measures are, or are believed to be, weak or non-existent. Furthermore, staff need to understand the consequences of breaches if they are to take their responsibility seriously.

Security officers should be encouraged and supported to speak directly with individuals who are conveying the wrong behaviours. This can range from 'soft' interventions such as questioning someone who's not displaying their pass, to 'hard' measures such as reporting an 'offender' to the head of security resulting in disciplinary procedures.

Speak to your Human Resources department for advice on punitive measures such as having an offence documented in an employment record.

'Stick'-like measures can contribute to security-savvy behaviour in your organisation. But they work most effectively when combined with the carrot of rewards or recognition for good security behaviour.

TIP: Make it real

Provide staff with real life examples of relevant poor security behaviours and their consequences. For example, prepare an intranet story about a security breach at an organisation similar to yours, the impact, and how it could have been avoided.

TIP: Embedding good behaviours in policies

You may want to consider how to write compliance measures into your organisation's security policy. Talk to HR about how to introduce vigilant security behaviours into staff induction, appraisals and personal development plans.

2 Guiding principles for a successful staff vigilance campaign

The fifth 'E' is for Evaluation

As security manager you will need to know if your campaign is working, to build upon successes and improve future communications.

Before you embark on a campaign, take a baseline reading of staff vigilance and reporting levels. You can then decide what you want to achieve and how you will measure progress.

The sort of things we suggest you baseline and measure over time are:

- Attitudes towards security including awareness of threat and risk
- Current security behaviour
  - Personal security
  - Vigilance levels
  - Propensity to report
  - Personal security practice: when online, and when entering and leaving your premises
- Awareness of security campaigns and communications
- Message take-out from such campaigns and communications
- Expected future behaviour
  - Likelihood to report
  - Greater alertness to suspicious behaviour
  - Personal security practice: when online, and when entering and leaving your premises

Measuring your campaign's input

We have tried a number of research methods from online surveys to staff interviews and focus groups and their success seems to be dependent on the organisation, its size and its practice as regards employee surveys. However, you may find it helpful to look at the example questionnaire in Annex C.

If you use questionnaires, decide on the most suitable method of distributing and collecting them based on timeframes, logistics, and the amount of data you want to collect.

You could conduct an online survey, email a questionnaire or – as we think works best – conduct short interviews with staff as they enter and exit the building. Response rates for self-completion surveys can be quite low so consider how to incentivise staff to complete questionnaires if adopting this approach. For example, hand delivery can make the difference to a colleague completing a form – but be sure to point out that responses remain anonymous.

Methods for collecting the questionnaires can include a 'voting box' in the staff room, stamped addressed envelopes sent back to the HR department/PO Box or using a third party to conduct the survey on your behalf.

It is important that results of staff surveys are triangulated with other data such as reports of suspicious behaviour (calls to the dedicated line etc.) and hostile reconnaissance. Also, interview colleagues in the organisation and members of your security team to find out their perspective. We have developed interview protocols which organisations can use; please talk to your CPNI adviser or your CTSA.

Being able to report success up the line will not only be important to demonstrate the value of running such campaigns but to ensure senior management continue to buy in to future campaigns.

Evaluation will help you plan future campaigns. It will show you clearly what to build on in the next iteration, so you can maintain momentum.

In the next section, we show you step-by-step how to run vigilant security behaviour change campaigns in your own organisation.

We work with a number of organisations who have followed this process themselves, to good effect. If you would like to see the results, please ask your CPNI adviser.

3 How to run a staff vigilance campaign

Through our work with a number of organisations, CPNI has developed the following steps to prepare and run a security behaviour change campaign.

Step 1. Gaining the support of senior management and internal communications colleagues

Step 2. Bringing together a team to deliver the campaign

Step 3. Developing your overarching strategy

Step 4. Developing and applying your project plan

We'll look in more detail at each step next. We have indicated when there are supporting materials available to help you with a step.

Step 1: Gaining the support of senior management and internal communications colleagues

The first step is to gain buy in from senior management and support from the internal communications team, if you have one. These colleagues will understand the best ways of communicating with staff and give you access to different lines of communication (e.g. staff newsletters, intranet etc). They also have control over which other campaigns are running internally. It is important to understand what else is planned to run, and when, as it may support or clash with the campaign you have planned.

As with the education piece previously outlined, this is about making both senior managers and internal communications personnel aware of the threat, the aims and objectives of your campaign and why it is essential to run this campaign. You may get some concerns over the potential to upset staff. To help with this discussion, you can draw on the fact that the campaign has been tried and evaluated by CPNI in a range of organisations, who have found staff respond overwhelmingly positively to these campaigns. There may also be concerns raised over the work needed to achieve this. Again, you can draw heavily on this guidance and toolkit, which directs you to materials that can be tailored by your internal communications department.

It is critical to recruit a senior management lead for the campaign during this step – someone who will be the visible champion and take ultimate responsibility for its delivery and, if required, report on progress to the board or CEO.

You can download a senior management briefing pack, containing notes to share directly with senior management, from our website.

Gaining support for your campaign

Your organisation's management and communications specialists may express concern about causing alarm amongst your colleagues. Explain that underlining risks will be combined with positive messages about the impact of a workforce with a unified approach to security. Invite their help with pitching your communications. Furthermore, our research with similar organisations has found that staff overwhelmingly respond positively to campaigns of this nature. See Annex B and D for more information and supporting materials.

If there are questions over the resources or manpower required to run a campaign, make use of the materials and frameworks contained in this guidance. You can tailor existing content, rather than invest a lot of time producing new content.

Ultimately, you will be making senior managers and communications colleagues aware of the threat, the objectives and why it is essential to run this type of campaign.

3 How to run a staff vigilance campaign

Step 2: Bringing together a team to deliver the campaign

Once given the go-ahead to proceed, the next step is to bring together a small team to successfully deliver and evaluate the campaign. The exact membership of the team will vary from organisation to organisation, but the following core membership is suggested.

Team member	Responsibility
Project manager	Someone needs to project manage on a day-to-day basis. This could be anyone with the right skill set within the team, e.g. the security manager or a member of internal communications.
Senior manager	Ultimate oversight; responsibility for delivery at board level; endorsing and championing campaign.
Security manager	Provides expert input from security perspective. Provides soundbites and information for articles, and facilitates access to security facilities and manpower where required (e.g. visits to control room, arranging for security officers to deliver wallet cards to staff etc.).
Internal communications representative	Determines timing of campaign; helps write and publish articles, newsletters, etc. Organises design and production of posters and other materials (e.g. wallet cards); advises on best delivery mechanisms for materials.
Staff/union representative	Provides expert input in terms of staff reaction to campaign, methods of delivery etc.

Step 3: Developing your overarching strategy

One of the first outputs from the campaign team should be a simple, agreed strategy from which a project plan can be developed. This does not need to be complicated. Indeed, it should be simple and clear.

To develop your strategy, address the following questions:

- Why are you undertaking a campaign? What is it you want to achieve? What is your vision?
- What are existing staff behaviours, good and bad, in terms of vigilance and reporting in?*
- How aware are staff of the threat to them and/or the organisation?
- Do staff know what suspicious activity is and how to report this immediately?
- What are the potential barriers or facilitators to staff undertaking the behaviours you want (e.g. uncertainty over what will happen to their report, their report not being taken seriously, no control room number on the staff intranet etc.)?
- What specific behaviours do you want to see as a result of improving awareness of employee vigilance and how might you measure this?
- What are the delivery mechanisms? How do staff like to receive their information – e.g. newsletter, intranet, briefings, special security awareness events. Can you cover as many as possible?
- Do you have contact with credible experts who you can bring in to support and endorse your campaign, e.g. a local CTSA?

*This is important as you may be fortunate enough to have staff who display good behaviour – in which case you need to acknowledge it in your campaign and encourage them to continue.

You may have enough expertise in your core team to answer all these questions or you may need to first embark on an internal data gathering and analysis phase. This may require consultation with others within your organisation (e.g. security officers, line managers) or running some focus groups with your staff.

A simple strategy is important as it will enable the core team to have a clear, shared and agreed awareness of the aims of the campaign and what needs to be done. This will help keep the campaign focussed.

3 How to run a staff vigilance campaign

(Step 3: cont.)

We suggest that your short strategy document should cover the following.

Section	Content
1. Overview	Current situation. What is the threat? Why do you want to run this campaign? What are current staff behaviours, good and bad? What behaviours do you want to change?
2. Aims and objectives of the campaign	For example: • Educate staff about the threat and their key role in protective security; • Staff to become self-aware and show the right 'security-savvy' behaviours in and around your site; • Staff to understand what may be suspicious activity, to be vigilant for this and report in to security immediately.
3. Key messages	What are the two to three key messages you want staff to take away as a result of this campaign? These are vital, as you need to embed and repeat these at every opportunity, e.g. in newsletters or intranet articles, in an email of endorsement from the CEO, through posters etc. Having these key messages will help keep everything you produce for the campaign focussed. The more you repeat them, the greater the chance of these messages really registering with staff (research shows people need to be exposed a minimum of three times to a message for it to begin to stick). Examples may be: • Whilst the threat to our organisation is moderate we cannot afford to be complacent. • We have a range of security measures in place to protect against threats, but you have a vital role to play in helping keep yourself, your colleagues and our site safe. • How you behave around our sites can have a huge impact on those who may wish to cause us harm – be vigilant and report in anything suspicious to security immediately.
4. The team roles and responsibilities	As outlined in Step 2 on page 20.
5. Overarching plan of activities	How you will deliver, mapped against the 5 'E's. This is a critical component of your strategy that will help you co-ordinate your activities effectively and ensure you are addressing the 5 'E's to maximise the likelihood of success (see the table below): • Education – how will you educate staff? • Endorsement – have you got the right people lined up to endorse the campaign (from inside and outside your organisation)? • Ease – can staff easily report anything they see that might be suspicious? • Enforcement – are your security officers briefed and authorised to challenge staff if they are displaying the wrong behaviours? • Evaluation – what are you measuring, when, why and how?
6. Success criteria and measures	Articulate what success will look like, how you will measure this, as outlined under 'Evaluation' in Section 2.

Research suggests that staff can be complacent about the threat, believing their organisation to be secure.

3 How to run a staff vigilance campaign

(Step 3: cont.)

Examples of how you can map the 5 'E's to your delivery mechanisms:

Example delivery mechanism	Education	Endorsement	Ease	Enforcement	Evaluation
CEO's weekly newsletter	Outline the threat and how staff behaviour can aid protective security	Staff have a vital role to play	Where to find control room number on company intranet	Has instructed security officers to have a polite word with those not showing right behaviours	
Intranet article on 'thinking like the enemy'	What hostile reconnaissance is. The effects, motivating and deterring, that staff behaviour can have on those conducting it	Credible external expert stating that the right staff behaviours can be hugely deterring			
Security manager blog or article	What are bad behaviours seen by security and why are these bad? What are good behaviours? Security measures are strong, but staff can help enhance this by being aware of their own behaviour, being vigilant and reporting in. What happens to a report from staff (real examples plus outcomes)?	Security officers themselves welcome your assistance and will treat any report in with due respect	Speak to a security officer or call the control room		
Security awareness event	Showcase all protective security measures in place for your organisation, e.g. visits to control room, meet the patrol dogs etc.	Security officers endorse campaign, convey to staff they have key role to play in assisting site security, welcome reports etc.			
Posters	What suspicious activity to look out for		Phone number on poster with reminder to report immediately		
Wallet cards	Reminder of what to look out for and to report in immediately		Phone number of control room to facilitate reports when off-site		
Security officers watching for staff behaviours				Quick, friendly but firm chat to those seen displaying poor behaviours around the site	Number and type of behaviours seen over time and response by staff to chats
Reports in to security					Quality and quantity of suspicious activity reports in to security control room
Staff survey					Short interviews with staff to ascertain if they've obtained key messages, how they felt about the campaign, and if they've changed their behaviours as a result

3 How to run a staff vigilance campaign

(Step 3: cont.)

Give yourselves the best chance of achieving behaviour change by getting the message out in a coordinated way. Think about how you can layer your communication by plugging into all your available internal communication channels as well as taking every opportunity to gather staff together for face-to-face briefings and workshops. Think creatively and laterally about how you can engage with employees.

Ideas that some organisations have used to good effect are:

- Lunchtime lectures by specialist speakers
- Team meetings
- Glossy magazine booklets desk-dropped
- Blogs by senior security personnel about outcomes of suspicious activity reports.

Step 4: Developing and applying your project plan

The next step is to get into the detail of the project plan. You need to consider three main phases – pre-launch activities, the launch itself, and post launch activities. For further information please refer to the case study 'Running a staff vigilance plus personal security awareness campaign' in Annex B.

Pre-launch – the planning and preparation of:

- articles such as informative pieces and FAQs for staff and managers
- team or management briefing packs
- posters and wallet cards; how these will be placed and distributed (see Annex E)
- content for the CEO newsletter completed in time for him or her to review and sign it off
- briefings for security officers prior to campaign launch so they know how to respond to any staff questions
- a security awareness event (if you intend to do this during the launch period this will probably need to extend your planning time).

Launch period – this starts from the moment the campaign becomes highly visible, i.e. when posters go up, wallet cards and/or guidance is desk dropped and the main education pieces go up on the intranet along with the supporting letter from the CEO. (Typically the posters should be up for approximately three weeks – no longer or they will start to fade into the background as staff become familiar with them.)

About a week into the campaign you could consider other activities to reinforce the message – for example, getting security officers to hand out wallet cards to staff as they enter or exit the site. Any staff surveys should happen towards the end of the launch period – i.e. 2-3 weeks from the start of the campaign, giving enough time for the messages to sink in and for staff to change their behaviour if needed.

Post launch – this is about keeping the 'drum beat' going. Punctuate the big impactful visual elements of your campaign with:

- a report on the outcomes of the campaign so far – how staff received it (e.g. interesting summary of the evaluation you are doing)
- regular security blog updates from head of security
- relevant public news articles to remind staff of the need to be vigilant and report in.

Annex A

Top tips for a successful campaign

1. Understand your organisation

What works and what doesn't in your organisation? How do staff like to be communicated with? Who are they most likely to respect as the 'voice' of the campaign?

2. Know what your desired behaviours are

Be clear as a group on the behaviours you are looking to change. And have a plan to find out if you have successfully communicated what the behaviours are and to measure if you have changed them.

3. A few key messages

Identify two or three key messages that underpin your communication and stick to them. Find out whether you have been successful in communicating them.

4. Coordinate and layer your activities

Give yourselves the best chance of achieving behaviour change by getting the message out in a coordinated way. Think about how you can layer your communication by plugging into all your available internal communication channels as well as taking every opportunity to gather staff together for face-to-face briefings and workshops. Think creatively and laterally about how you can move employees in the right direction.

Ideas that some organisations have used to good effect are:

- Lunchtime lectures by specialist speakers
- Team meetings
- Glossy magazine booklets desk-dropped
- Blogs by senior security personnel about outcomes of suspicious activity reports.

Don't assume you know best how to reach staff. Ask them!

5. Build in the 5 'E's

- Education – how will you educate staff?
- Endorsement – have you got the right people (from inside and outside your organisation) lined up to endorse the campaign?
- Ease – can staff easily report anything they see that might be suspicious?
- Enforcement – are your security officers briefed and authorised to challenge staff if they are displaying the wrong behaviours?
- Evaluation – what are you measuring, when, why and how?

Annex B

Including personal security advice in your campaign

If you have intelligence or concerns that staff themselves may be a target you will want employees to think about their own personal security on top of staying vigilant and reporting suspicious activity.

Below, we show you how to run a staff vigilance and behaviour change campaign with a strong focus on personal security (i.e. the specific measures and behaviours staff should undertake to stay safe and reduce the risk of becoming a target).

You should still use the steps outlined in Section 3 of this guidance for your campaign. But the following advice will help you to place greater emphasis on personal security. We also direct you below to template communication materials that are particularly relevant to personal security. For example, guidance booklets, wallet cards, supportive notices from senior managers, intranet articles and blogs.

What to say

What is important to consider from the start is the strength of the threat, how concerned you are about it and how much you want your staff to adhere to what you are asking them to do. For example, if there is a non-specific threat (e.g. a general increase in threat level) then you may want to run a campaign as outlined in Section 3 and simply start to introduce the aspect of employees considering their own personal security.

If, however, the threat is specific to your organisation or you have significant concern that your staff may be targeted themselves, then you may wish to run a campaign that is harder hitting in terms of its messages, and which makes very clear the actions staff need to take.

Whatever your stance and aims, first of all, you need to contextualise the threat. This may mean relating it to a general threat, such as a heightened response to international terrorism, or it may be a specific security threat your organisation faces. Try and describe how this threat might play out in terms of targeting staff and why they would want to do this. This will help staff identify suspicious activity and be mindful of their own behaviour, as well as that of colleagues.

Second, communicate the measures your organisation has in place to safeguard staff – both hard and soft- in response to this particular threat. You might want to talk about your physical defences, technical assets and internet controls here. You might want to refer to how you are widening your security footprint using a combination of CCTV, foot patrols and staff vigilance. In a similar vein you may want to highlight how you integrate your security with local police forces and any 'organisation-watch' schemes you and like-minded organisations are part of.

Stress that whilst you are doing everything you can to help keep the organisation safe in response to the particular threat, staff have a vital role to play by:

- being vigilant
- reporting in suspicious activity immediately
- undertaking their own good personal security practices.

You can help employees achieve this by providing advice and guidance about their personal security, the simple steps they can take online, their journey to work and approaching and leaving the site. Provide them with CPNI's Personal Security Guidance documents, which will help explain why it is important they consider their personal security and the easy steps they can take. These are available to download from our website.

In terms of their personal security online, remind staff of the risk posed by personal information on the internet – especially if it associates them easily with their place of work.

Tell staff exactly what is required of them. For example:

- Looking alert continuously during their commute
- Not taking the same routes to work
- Ensuring passes are put away immediately on exiting the building and are not on show outside the building in any way
- Not wearing company-logoed clothing (e.g fleeces, polo shirts, fluorescent jackets) outside of the site where they are not required
- Not being on their phones as they enter and leave sites
- Not having headphones on as they enter and leave sites
- Not smoking in the immediate vicinity of the building
- Regularly checking their privacy settings on social media sites
- Not talking about work online
- Changing their profile picture to something less identifiable
- Understand what information is available about them online
- The need to be vigilant, act vigilantly and report in anything suspicious to security immediately.

Our example intranet pages and personal security guidance advice, downloadable from our website, can assist you with this. Think too about how you communicate the message in terms of tone of voice; on the one hand you want staff to sit up and listen but on the other you want to avoid unnecessarily alarming them. Getting the balance right can be a challenge so anything you can do to suggest to staff that you are supporting them in keeping themselves safe can go a long way. For example, we developed a personal security plan for an organisation and communicated it using a catchy mnemonic device; see below.

Annex B

Introducing P.I.P.P.A. – Your 5-point personal security plan

The best way to implement your P.I.P.P.A. personal security plan is with "joined up thinking". Your home, work and online lives overlap.

So you should not prioritise securing one area over and above the others.

Plan
Think about likely threats and what you would do if they happened. Plan contingency travel arrangements and keep emergency contact details easily accessible.

Information
Keep your private information private. Most targeting is initially done online. Think about what you put on the internet and use good IT security practices.

Predictability
Avoid predictable routines, especially during enhanced periods of vigilance. Be aware of fixed times, locations and routes in your day. Vary them as much as possible.

Profile
Be aware of your environment. When leaving a location, take in your surroundings. Act confidently. Looking less like a target makes it less likely hostiles will target you.

Anonymity
Do not publicise who you are. Try not to link home and work life and be aware how snippets of information can be combined to create a full, exploitable picture of you.

Remember: report anything you think is suspicious. In doing so, you are helping ensure your safety and the safety of those around you.

If in doubt, call...
Together, we've got it covered

Case study: running a staff vigilance plus personal security awareness campaign

The aim

An organisation worked with us to test and evaluate this type of staff vigilance and personal security campaign strategy. In response to a recent increase in the general threat level, this organisation wanted staff to display more 'security-savvy' behaviours around the site, be vigilant of suspicious activity and report in immediately. However, it also wanted to introduce staff to the concept of their responsibility for their own personal security; to start to embed this idea now in case a specific threat emerged. It wanted to achieve this whilst not unduly alarming staff.

The campaign

Following the steps outlined in Section 3, the organisation ran a staff vigilance behaviour campaign over the course of a month. A range of delivery mechanisms were used, including a security event and communications (which we have redacted and provided as downloadable examples on our website).

Posters were placed at optimal places in the site such as security notice boards, lifts and – most effectively – as large pop-up banners where staff entered and left the building. The personal security guidance was made available on the staff intranet and a few days after the initial launch, P.I.P.P.A. wallet cards were desk-dropped by security officers during their normal overnight patrols of the office.

There were two key metrics of success: significant increase in suspicious activity reporting into security; and improved staff attitudes and opinions with regard to their security behaviours (as obtained from a short interview survey).

Results

Reports into security increased five-fold, including reports from visitors as well as staff. These were also good quality reports in terms of the detail provided. One of the reports led to a police investigation – the outcome was that the suspicious person was a pick pocket. The head of security used this report and example in one of his blogs to clearly show how seriously reports are taken, what happens to them and outcomes. While the individual was, in this case, a thief they could easily have been a more significant threat.

Short interview intercepts with 86 employees showed that:

- 94% were aware of the campaign and found it useful
- 66% reported that they had changed (improved) their security behaviours in terms of vigilance and personal security
- 64% stated that they were more likely to report anything suspicious to security
- 63% felt reassured or safe as a result of the campaign (i.e. that the organisation was taking the security of its staff seriously).

Analysis of anecdotal comments found that those who stated they have not changed their security behaviours or were not more likely to report anything suspicious to security believed they did this already. The research therefore indicated two groups of employees: those for whom the campaign reinforced their current (self-perceived) good security behaviours and those who have been moved towards undertaking the desired behaviours.

Annex B

As such, the conclusion was that the ongoing campaign should keep to the same key messages and tone of voice. The research also showed that the intranet was the least preferred method of delivery of the campaign (74% liked the posters, 57% wallet cards and 32% the intranet). However the intranet was the only source of the vital education aspect of the strategy; the 'why' employees were asked to think about and change their behaviours.

Next steps

Next, the campaign will continue to provide a 'drum beat'. A set of coordinated activities across a variety of delivery mechanisms will educate staff and convey the key messages without relying on the staff intranet.

This includes induction training, blogs by senior security personnel about the outcomes of suspicious activity reports, lunchtime lectures by security specialists, utilising team meetings and using different kinds of materials in desk drops.

It will also include a more active role for security officers who will speak directly to individuals who are conveying the wrong behaviours and making staff aware of this activity.

A major refresher of the campaign is scheduled to take place six months after the initial campaign; timing that was perceived to be about right by the employees surveyed.

Annex C

Evaluating your campaign

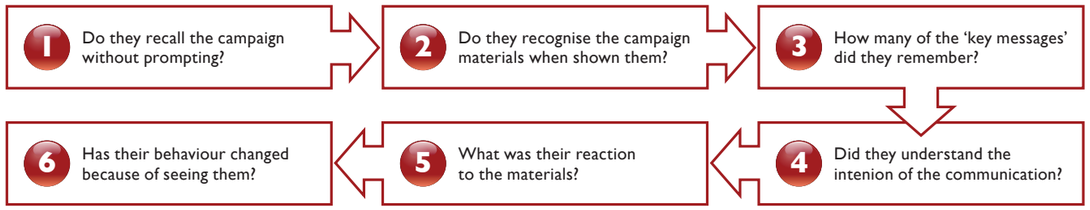
After the campaign has been launched for a while, it's a good idea to evaluate how well it's working. Speaking to members of staff will give you a good sense of staff awareness of the campaign and their perceptions of its impact on behaviour, as well as which elements of the campaign have been most successful and anything which hasn't worked so well.

Measuring effectiveness using a staff survey

The reception of staff is crucial to the success of the campaign and understanding their response can help you to fine-tune and target the campaign more effectively.

A five-minute questionnaire can help assess whether your campaign materials have been seen; what message staff took from them; and whether or not they have had the desired impact. The larger and wider the sample the better, so try to speak to as many staff members as possible from a range of departments, including a mix of males and females and a range of ages. Ideally, questions should combine a numerical or quantitative element (i.e. "Yes" or "No" questions that can be turned into a percentage) as well as subjective or qualitative elements, which seek more general opinions.

Here are the key questions you can ask site users:



Here are some example questions you might like to include in your survey:

Question area	Example question	Response type
Demographics (n.b. if you have a small number of staff, demographics can potentially help to identify individuals and may lead to them being less candid in their response.)	Q. Job title:	Quantitative
	Q. Age:	Quantitative
	Q. Department:	Quantitative
	Q. How long have you worked for the organisation?	Quantitative
Warm-Up/Scene setting	Q. What do you think the main security risks are in [insert site name]?	Qualitative
	Q. What security measures are you aware of being in place at [insert site name]?	Qualitative
Awareness	Q. Are you aware of any current security campaigns in place at [insert site name]?	Quantitative
	Q. If yes, what have you seen?	Qualitative
	Q. Have you noticed any of the following: a) posters b) intranet pages c) wallet cards [replace with any communication channels used at your organisation] [use visual aid showing materials]	Quantitative
	Q. Which messaging format(s) did you find most helpful? a) posters b) intranet pages c) wallet cards [replace with any communication channels used at your organisation]	Quantitative
	Q. How did you first hear about this security campaign?	Qualitative

Annex C

Question area	Example question	Response Type
Message take-out	Q. What do you think the campaign materials are trying to say?	Qualitative
	Q. Who do you think the campaign materials are aimed at?	Qualitative
	Q. How does the campaign make you feel?	Qualitative
Effect on security behaviours	What impact, if any, has the campaign had on your vigilance and alertness regarding the behaviour of others?	Qualitative
	What impact, if any, has the campaign had on your likelihood of reporting anything odd or suspicious to site security?	Qualitative
	What, if anything, have you changed about your own behaviour as a result of the campaign?	Qualitative
Running a security campaign	Have you found the security campaign useful?	Quantitative
	How often do you believe the organisation should run campaigns like this?	Quantitative
	Do you have any other comments to add about the campaign or personal security in the organisation?	Qualitative

Each question will tell you something different about how to optimise the materials at your site:

1. If large numbers do not recall the campaign, you should review how visible the campaign materials are and the format they are distributed in.
2. If significant numbers still do not recognise the materials, you might need to produce more and to reconsider how they can be more effectively launched.
3. If significant numbers do not understand the key messages, there may be an issue with layering. You should make sure to use the full range of materials.
4. If your audience doesn't understand what the campaign is trying to achieve, it's worth shifting the balance towards more education pieces and long copy versions of the materials, which offer more explanation.
5. In the unlikely event that large numbers of staff are alarmed by the campaign, it's worth replacing some of the harder key messages with softer versions.
6. If staff have become more aware of their own behaviour and the behaviour of others, then the campaign has had the desired effect on site users. Remember, before you start it is worth discussing and determining what success should look like within your organisation.

TIP: Think about where and when you ask staff questions

It can be effective to intercept staff at a point where they should be displaying vigilance, e.g. when they are entering the building. This can reinforce the messages of the campaign.

Annex D

Supporting material for staff vigilance behaviour campaigns

The following material can be downloaded from the CPNI website:

Internal vigilance briefing

Introducing P.I.P.P.A.

Briefing pack for senior managers and team leaders (to describe the campaign and assist them with briefing their staff)

Example letter to endorse the campaign from a member of the board

Example security manager blog posts

Example intranet pages including staff FAQs

Personal security guidance (full version and leaflet)

Personal security briefing pack

Example wallet card

Staff vigilance behaviour posters

Further CPNI resources

The following guidance materials are also available on the CPNI website or via your CPNI adviser or CTSA:

Communicating Personnel Security Messages

Understanding Hostile Reconnaissance

Social Engineering: Understanding the Threat

Deterrence Communications

Security-minded Comms

Guard Force Motivation

CPNI – Threats to National Security

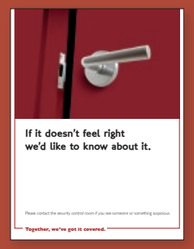
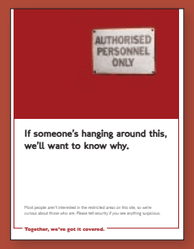
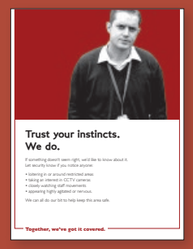
Annex E

Staff vigilance behaviour posters

We have created a suite of posters which organisations can use around their premises. The posters readily convey that security is everybody's business and empower staff to report suspicious activity.

There are 6 executions. Each covers a different aspect of site infrastructure. They range from harder messages to softer, more human, ones. So you can pick and choose the materials relevant to your needs. Higher security locations or CNI sites may want to consider a harder execution. For a more open site, such as a shopping centre, softer executions may be more appropriate.

Harder → **Softer**

Camera	Door	Sign	Dog	Team	Employee
					
Security cameras are a visible and important part of security. Taking an interest in the cameras could be suspicious. These posters are best placed near a security camera.	Staff are familiar with their surroundings and likely to spot anything out of place. Although this works best in an office situation, sited on or near access doors, it can be used anywhere where staff could be on the look-out for unauthorised access.	Someone loitering around a restricted entrance could be planning or waiting for an opportunity. Therefore, this poster should be placed near barriers to authorised areas, such as gates and doors.	There are many visible security assets on site including the use of dogs, but staff play an important role as well. Place these in areas where staff would expect to see surveillance equipment.	Similar to the 'Employee' poster, staff individually and collectively have a part to play in security. The posters are best placed in communal areas such as break rooms and canteens.	All staff have a part to play in security and any reporting will be taken seriously by the security team. Place these posters in communal areas and on notice boards.

Annex E

Together, we've got it covered.

These posters address your employees. 'We' (the organisation) give advice to 'you' (the employee) about what 'they' (hostile individuals) might be up to.

However, the executions also have a deterrent effect on any individual with bad intentions who might come into contact with them. They have been designed based on principles of deterrence communications and research into how hostile individuals conduct reconnaissance.

They use stylised imagery relating to security procedures and staff vigilance. This shows anyone who is up to no good that people will be scrutinising their behaviour.

To balance this deterrent effect, the headlines are carefully worded to reassure and empower staff. All materials also conclude with a warm, positive tagline: 'Together, we've got it covered.'

Customising the posters:

The posters can be easily tailored to your organisation by using your own branding and house-style, photography and call to action. Although some organisations prefer to use their own house colours for the posters research has shown that a red background tends to command attention in a security environment.

If you have a design capability in-house, talk to them about how to adapt and produce the materials. Alternatively, you can use your local graphics agency.

Refreshing the posters:

To keep the posters fresh we recommend that you change the copy every few months. This will improve uptake of the messaging.

Staff responses to the posters:

So far the poster materials have been used across 15 organisations, from closed sites (such as a power station) through to open locations (such as a shopping centre). Surveys to assess employees' responses to the communications found high numbers of staff demonstrated awareness of messaging around vigilance. Asked 'What do you think the material is saying?' 83% answered, be vigilant. Asked what effect the communications had, 62% said they would be more vigilant and 58% said they would be more likely to report.

TIP: High impact locations

Consider the use of large banner posters in entrances and exits to your buildings. This will remind staff, at the point that they enter or leave, to be vigilant and report in suspicious activity.