Security messages for new joiners

During the first 12 months of the employee lifecycle

CPNI
Centre for the Protection of National Infrastructure

CPNI

Centre for the Protection of National Infrastructure

This guidance has been designed to support security managers, hiring managers, and others in your organisation responsible for inducting new joiners, to best communicate your security policies, processes and ways of working. It is based on expert knowledge as well as CPNI research on induction processes within UK Critical National Infrastructure (CNI) organisations and provides exercises to help you to shape what security messages to give, when, and how, during the first 12 months of the employee lifecycle.

Overview and aim of this guidance

Developing and maintaining an effective security culture is a key element of an organisation's protective security regime. The mind-set and behaviour of your employees (including contractors) can have a real impact on the security risks and vulnerabilities your organisation faces. Security breaches of any kind can result in loss of revenue, productivity or share price; they can damage an organisation's reputation and morale; they might result in confidential data being leaked; or worse, they can result in physical harm to employees or the public.

Security awareness is integral to all stages of the employee life cycle[1]. However, the induction of new joiners is a key first point at which their perception of security in the organisation is formed. This stage provides the organisation with an opportunity to embed the desired security mind-set and behaviours from the outset.

For the purpose of this guidance, security messaging relates to any communication from an organisation that is intended to disseminate security information to its employees, either to influence relevant security behaviour or to instil awareness of a security policy, issue or threat.

[1]The 'employee life cycle' is a well known concept – it represents all stages of the employment relationship. It begins with recruitment and 'on-boarding' (the stage where induction occurs), and runs all the way through to performance management, transfers, promotions and leaving the organisation.

"Developing and maintaining an effective security culture is a key element…"

Table of
CONTENTS

This framework is divided into five sections to support you as you consider how to engage your employees with the security messages they need to know to keep your organisation secure.

01

Security

Making security meaningful for new joiners

New employees joining your organisation will have varying levels of experience with security as a concept. They may not be aware that behaving in a security conscious way is important in their new workplace. Therefore, as a first step in inducting new joiners it is essential to define exactly **why security is important to your organisation.**

A good way of communicating this is to highlight your organisation's core mission and the assets to keep secure. Organisations in the CNI may face a range of threats due to their core mission and critical assets being integral to the UK. Therefore, it is vital to have appropriate security practices based on the range of threats your organisation faces. With this in mind, you can work with new joiners to discuss the threats and the impact a potential security incident could have on your organisation. Make use of up-to-date threat information wherever possible.

This approach will help new joiners to understand the context for why they need to develop a security conscious mind-set and follow the organisation's security policies and procedures. Inducting new joiners in this way provides a firm foundation for their later learning as well as gaining their buy-in for supporting the organisation's security goals as part of their everyday work activities.

At this early stage you may like to develop your new joiners' understanding of the part they can play in keeping your organisation secure given the roles they have. Depending on the role of the new joiner, security may be relevant in different ways and to varying degrees. For example, based on your organisation's risk assessment of sensitive posts, new joiners entering such roles may need additional security messages to emphasise the critical importance of being security conscious and the negative consequences if they are not. For outward facing roles such as reception staff and PAs, you may need to explain the threat from social engineering to reduce their vulnerability to inadvertently giving away sensitive information.

Therefore, making security meaningful by tailoring the message to their roles will assist new joiners with understanding how their actions have a direct consequence on the security of the organisation.

Exercise 1

Making security meaningful for new joiners

Based on the principles outlined in this section, we have developed this exercise to help you to design security messages for your new joiners. This exercise will help to define your core mission and the assets you need to protect, the threats and risks facing your organisation, and the part your employees can play in helping to keep the organisation secure.

You can use this structure to design briefings to new joiners. Alternatively, you could run an exercise with your new joiners to encourage them to generate their own examples. This may allow your new joiners to organise their thoughts in a way that is meaningful to them, and therefore easier for them to remember.

What is the core mission of the organisation and why is security important in the delivery of this?

What are the threats and risks facing the organisation?

E.g. physical attacks on sites or staff, cyber attacks on corporate IT systems, manipulation of staff to extract information, insider threat, accidental breaches of physical assets or information.

What are the key assets that need to be kept safe and secure from the range of threats and risks facing the organisation?

E.g. materials, equipment, customer and/or staff data, intellectual property, processes, systems, people, buildings, organisational reputation.

What part can those you are briefing play in keeping the organisation secure?

How can you tailor the message about why security matters to the employees you are briefing?

Notes:

02 New Joiners

What new joiners need to know and do to be secure

Once your new joiners are bought into why security matters, it is important that they learn how their **individual behaviours (both in and outside of their place of work) can support the organisation with keeping sensitive assets secure.**

At this early stage, new joiners may not yet appreciate exactly what types of security behaviours are expected of them. Therefore, you will need to ensure your new joiners are briefed on all the relevant security behaviours and practices that you'd like them to follow. Some of these may be applicable to all employees, others may only relate to particular roles, teams or locations (e.g. sensitive posts, management roles or a secure site). Make sure you are clear on who needs to be briefed on what.

There are potentially many behaviours that new joiners will need to learn about. Bear in mind that it will be important not to overload them with too much, or irrelevant, information at any point. There are some security practices that new joiners will need to be familiar with almost immediately, such as the need to display a security pass while on site and remove it from view when leaving the site. Awareness of other practices may not be needed from this early stage, e.g. security policies relating to overseas travel.

Some of the security practices you ask of your new joiners will be simple and 'clear cut', such as the rules regarding passes. Others may be complex and subtle and therefore could be more challenging to communicate and learn – e.g. the reporting of unusual/suspicious behaviour in the workplace. These more complex behaviours will require employees to draw on their experience and judgement in deciding the required course of action. You may like to take these differences into account when determining when and how employees should be educated in these areas. This is covered in detail in the next section.

Exercise 2

Relevant security behaviours and practices for new joiners

The following exercise sets out a number of contextual themes where new joiners may need to be briefed on the security behaviours and practices expected of them – e.g. what to do when entering and leaving sites, managing visitors, or using corporate IT. Use this exercise to identify what your new joiners will need to know and do in order to be security conscious in each of these areas. When you are completing the exercise, consider whether there are additional behaviours that new joiners need to understand that are specific to your organisation.

When completing this exercise you may find it useful to refer to CPNI's 'Small actions, big consequences: A framework for CNI organisations on security savvy employee behaviour'. This is a technical document for security managers (and others internally) that provides examples of effective and less effective security behaviours that CNI employees should adopt. A booklet containing these behaviours in an informative and engaging way has also been developed for employees, should you wish to share this with them (see page 39 in this guidance for further information on this product).

Relevant security behaviours for new joiners

Entering and leaving secure sites

E.g. entry/exit procedures, working out of hours, signing in and out, gaining entry if you have lost your pass, report suspicious behaviours around site.

In and around the workplace

E.g. pass wearing, clear desk policy, information storage, reporting of suspicious behaviours, remote working policy.

Managing visitors

E.g. signing-in procedures, escorting of visitors, visitor access to various parts of site.

Using corporate IT

E.g. locking unattended devices, password policy, using authorised removable media, using work devices appropriately, reporting suspicious email.

Representing the organisation online

E.g. gain approval before publishing or commenting online as a representative, ask the security department to review for any sensitive information.

Handling queries from customers, suppliers, partners or the public

E.g. awareness of social engineering tactics, check for sensitivity before sharing information, verify identity before sharing information.

Being a security advocate as a manager

E.g. brief team on security threats, check security knowledge levels of employees, encourage reporting of security concerns.

Life outside of work

E.g. what information can and cannot be shared with friends, family and contacts outside of work, behaviours in social situations such as team events.

Travelling overseas

Follow your organisation's travel policies and travel security advice.

Other behaviours

Any security behaviours specifically relevant to your organisation.

03 Communication

When and how to communicate these security messages

The earlier sections of this guidance outline the ‘why’ and the ‘what’ of developing new joiners’ understanding of security in your organisation. Continuing with the process of designing your security messages, it is important to also consider **‘when and how’ to deliver these.**

This section draws upon expert knowledge in training and learning, as well as research CPNI conducted within the CNI on induction processes. Some key ideas to bear in mind when planning when and how to deliver your security messages are provided in the following sections.

ONE

A 12 month timeframe

Utilising a 12 month timeframe to deliver security messages to new joiners allows for a structured programme, spread throughout this period. You need your new joiners to engage with security over the course of their employment with you in order to become security savvy employees. This approach can be undermined if security messages are delivered as a one-off brief at the very start, competing for attention amongst all of the other induction messages your new joiners will receive.

What do your new joiners need to know and do in terms of security by day one? How are you expecting them to behave in terms of security at 3, 6, 9 and 12 months? Thinking about your security messages in this way allows you to deliver them at relevant intervals for your new joiners.

A structured new joiners programme where your security messages are spread over the first 12 months reinforces the idea of continuous security education. It will support you in fostering the security savvy mind-set and behaviours in your new joiners from the outset.

TWO

Avoid overburdening

New joiners on induction programmes commonly feedback that they feel overburdened with too much information, both in volume and variety, that is delivered as soon as they join an organisation.

In secure organisations, recruitment and vetting processes can mean that new joiners have often had a long wait to join, and so the first few days can be crucial in generating their sense of identity and attachment as a new member of your organisation. A wide range of major organisations now focus more on creating an experience to welcome new joiners rather than overburdening them with too much information.

You can challenge the assumption that induction has to be 'learning a bit about everything'. When you design your security messages ask the questions: do new joiners really need this information now, in the first few days? Or do you risk overburdening them?

THREE

Layering of messages

CPNI research highlighted that security managers recognise that a highly effective method to communicate security messages is to 'layer' these over time and to build up from simple security behaviours to more complex behaviours. For example, some organisations conduct 'security refresher' training with new joiners around 6 months after receiving the initial security messages. This approach is intended to elaborate on security after new joiners have had some experience in the organisation.

This layering approach fits in with the principle of not overburdening new joiners and ensures that security knowledge and awareness is developed more fully over time. In layering your messages, take care not to bombard new joiners with unnecessary or repetitive updates, otherwise they may pay less attention to future security messages and become disengaged. Aim to communicate with your new joiners only when you have relevant or salient security messages to deliver.

FOUR

Tailoring

Organisations often report that initial security inductions need to be general in nature to ensure that they are immediately applicable to as many employees as possible, due to the variety of roles within the organisations. Taking this 'catch-all' approach can be beneficial; it reduces the burden on those delivering security messages and ensures that you reach the widest possible audience. Some organisations have even introduced online training-based inductions in an effort to standardise the quality, length and time given to critical security messages.

However, be mindful that the downside of the generic approach is that some security messages may not be relevant to the whole audience. For example, new joiners without a need for IT access may be frustrated to receive in-depth sessions on corporate IT security policy. It also limits the extent to which you can adapt key messages to suit your audience and maximise their impact. As outlined in the 'making security meaningful to new joiners' section of this guidance, there may be specific roles within your organisation that would benefit from tailored security messages. Where possible, look for opportunities to do this.

Finally, try to design your security messages to appeal to your new joiners' sense of 'what's in it for me?' For example, highlighting how a security behaviour will help to keep them and their family secure, as well as the organisation, is a good way of engaging new joiners (e.g. the benefit of good online security practice which enhances online security at home as well as at work). If you can encourage new joiners to adopt positive security behaviours in their personal lives, then these may transfer into the way they behave in the workplace.

FIVE

Appealing communication tools

In designing your organisation's security messages, try to avoid the potential pitfall of leaning too heavily on your organisation's security policy to convey the information to new joiners. Use more engaging methods of covering the appropriate content.

Learning is facilitated when educational materials are designed to appeal to multiple senses, such as vision, hearing, and touch ('doing'). Individuals will also differ in their preference for how information is presented and taken in, depending upon their own learning styles, personality and background. For these reasons, you should consider varying the medium by which security messages are delivered.

For example, delivery could be by face-to-face briefings, written briefs, animations, videos, quizzes, interactive tools, discussion groups, etc. It is likely that some communication will take place as part of a formal induction course, but there may be other opportunities for effective engagement within your organisational setting. Even small activities at the beginning of classroom presentations or workshops may be a useful way of getting new joiners engaged. For example, you could use CPNI's 'What kind of security agent are you?' (which forms part of the 'Workplace behaviours' campaign) or the 'Social engineering quiz' (which forms part of the 'Be savvy about the social engineer' campaign) as light hearted, interactive exercises to introduce new joiners to a topic or refresh previous training as an ice breaker exercise.

Remember that your new joiners may have time in their new roles which they can use to consolidate and absorb your security messages. You can signpost other resources such as e-learning, webpages and additional talks/workshops which can be followed up in their own timeframe.

Some organisations introduce an element of assessment to ensure new joiners meet a baseline of security knowledge having been through the induction programme. Introducing questions, quizzes or tests in this way can help to keep employees engaged and to ensure key points are taken in.

SIX

Using credible experts

Cross-departmental collaboration is important for communicating security messages – it is not just the role of the security department. Bringing in experts from across your organisation can reduce the burden on security teams of delivering security messages to your new joiners. Involving the communications, HR, legal, learning and development, line and senior management functions of your organisation will ensure that your new joiners receive consistent security messages. This approach also reflects positively on your security culture, as it shows new joiners that security is taken seriously and is valued by employees across your organisation.

The person delivering your security messages will also make a difference to how well they are received and understood. Credible experts (i.e. those that have a depth of knowledge of the subject matter) will be taken seriously and be considered to be valid 'role models'. One definition of learning is that it involves a change in attitudes/beliefs, knowledge and behaviour. Expert instructors are often the most effective at tackling the attitudinal aspect of this process. Conversely, those who have only a surface level of knowledge about a security topic may not be taken seriously by your new joiners, e.g. presenters of digital footprint guidance who are not familiar with modern usage of social networking sites and their privacy settings.

SEVEN

Engaging with line managers

Organisations cite the reinforcement of security messages by line managers as integral to the induction of new joiners. During the first 12 months, a new joiner may be more likely to raise a security issue with a line manager in the first instance rather than reaching out to the security department.

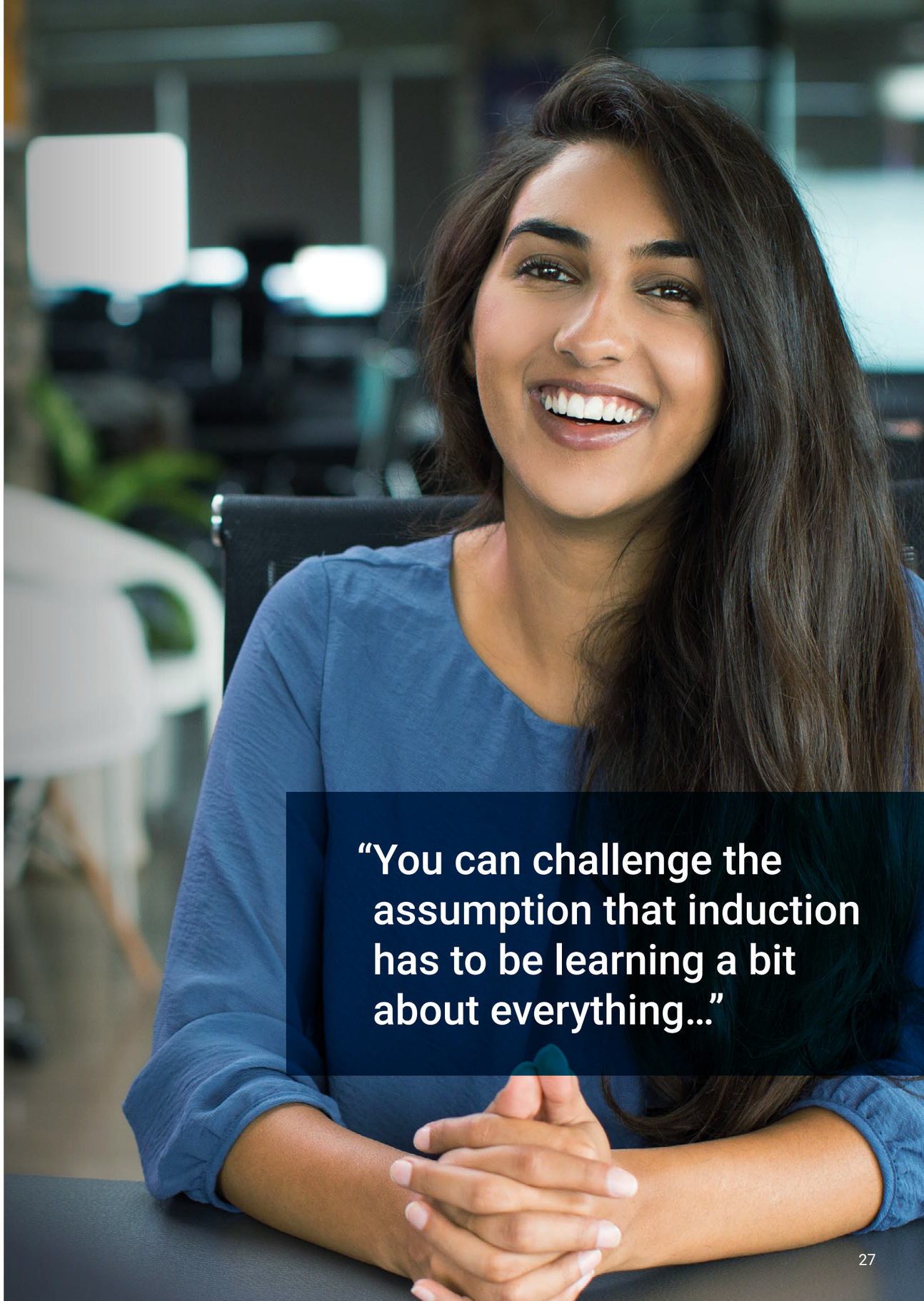
Therefore, there is extended value in engaging with line managers. Ensure that they understand their security responsibilities and know when it is appropriate to escalate security issues to the relevant contacts within your organisation. CPNI's 'Line managers' campaign may help you with this (see page 38 of this guidance).

EIGHT

Including senior managers

The way seniors behave has an important influence on your organisation's security culture. If the security practices are not visibly supported by senior leaders, then this can significantly undermine any good work undertaken by the rest of the organisation to promote positive security behaviours. For new joiners coming into senior positions it is therefore critical that they receive the same security messages as other new joiners. This reinforces that security is important for everyone in the organisation and it is everyone's responsibility.

Ideally, senior managers will also receive a separate briefing on the important role they play in setting and maintaining a strong security culture. You may need to tailor the security messages you deliver to suit the availability and time constraints of senior personnel. In these instances, getting the relevant support staff (e.g. Secretaries, PA staff) on-board with the security messages can be invaluable in supporting you with delivering your security messages (indirectly) to senior managers.

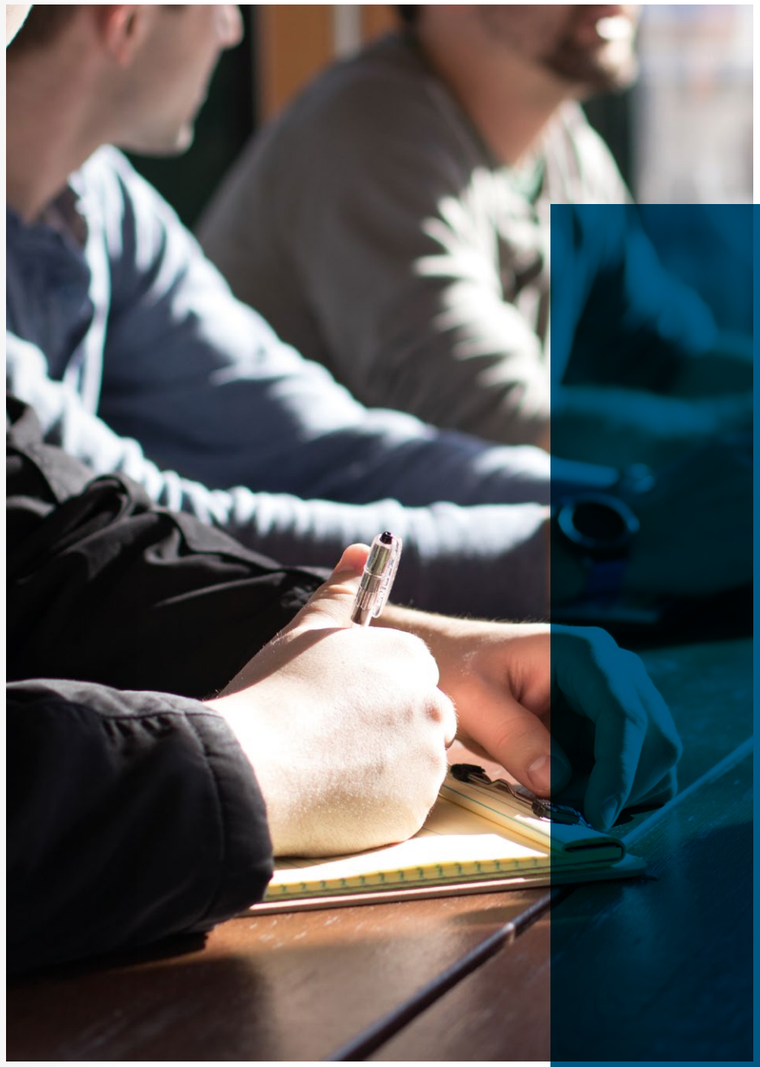


NINE

Leaving a lasting impression

Security messages delivered on induction can sometimes be too heavily focused on the technical countermeasures to mitigate security threats. Instead, it may be helpful to encourage new joiners to think about security in its broadest sense (i.e. what employees and visitors do, as well as the physical and technical measures in place). This will help to get away from the concept that security is done by others (i.e. gates, IT firewalls and guards in hi-vis jackets). What would you like your employees to think about when they hear the word 'security' in your organisation? Cultivate this mind-set and outlook with your new joiners. Put across the message that security is an enabler and not a barrier to getting work done.

Work with your communications team to review and reflect on how you would like to position the security department within your organisation. Would you like to have an authoritative style or be seen as an approachable and consultative team where employees are encouraged to contribute to the development of security practices? Think about the brand and image you portray to new joiners – the approach you take to delivering messages about security is an important part of this. This is your opportunity to leave a lasting impression so make the most of it.



Exercise 3

When and how to communicate these security messages

This exercise has been designed to help you to consider when security messages should be delivered, how and by whom within your own organisation. Your outputs from Exercise 2 will provide the foundation for the core content of your security messages.

Useful questions for you to consider when completing this exercise may include:

- What do employees need to know very early on in their employment with you?
- Which security messages can wait until later on in the 12 month period?
- Which security messages will you need to reinforce or repeat over the 12 month period?
- How simple and straightforward are the behaviours to communicate and for your new joiners to understand and demonstrate?
- Do you have the resources within your organisation to use your chosen delivery method?
  (e.g. face-to-face presentations, training courses, e-learning, posters/hand-outs/wallet cards and other printed media, animations, videos, quizzes, intranet articles, discussion groups, mentoring).
- How accessible are certain resources (e.g. online access, e-learning platforms) to different groups of new joiners?
- Which areas of your organisation will need to 'buy-in' to your security messaging programme?
  (e.g. learning and development, communications, HR, line managers, senior managers, security department).

Exercise 3: Example Table

Theme	Week 1	3 Months	6 Months	12 Months
Example: Communicating the threat	Security deliver an interactive exercise. New joiners populate what they think the threats facing organisations are.	Security messages disseminated to all employees via quarterly security newsletter: threat updates...		Comms team support to produce annual update on threats on intranet. Links to the relevant security behaviours to help mitigate the threat.
Example: Entering and leaving secure sites – pass procedures	Pass office to deliver face-to-face session: – Allocate security pass – Explain different pass types...			
Example: In and around the workplace – working from home	New joiners are signposted to the remote working policy to consult when needed in an induction briefing by HR.		Line manager briefs new joiner on remote working policy before they get permission to work at home.	
Example: Digital footprints	Security department to introduce concept of digital footprint: what it is, who can add to it and that the individual should actively manage it.	E-learning module to train new joiners how to actively shape their digital footprint and introduce resources for them to do it...		Annual refresher on Intranet to remind employees of the need to continually manage their digital footprint.

The above table illustrates some examples on how you may want to use the exercise – it is not meant to serve as a definitive or exhaustive list. We would advise completing this exercise in an Excel document to plan out each week/month.

04

Evaluation

Evaluating your security messages for new joiners

Once your security messages for new joiners programme is up and running, you will want to measure how well it is working. Surveying your new joiners can be a quick and easy way to evaluate. A quick questionnaire as and when new joiners receive your security messages can help to check:

- Can they recall the key security messages they received?
- Did they understand why the security messages were relevant to keeping the organisation secure?
- Was the content pitched at the right level? (e.g. too difficult to understand or too much/not enough detail)
- Do your new joiners have ideas for how the security messages could be delivered? Is there anything you can do to make them more engaging or appealing?
- What impression of security and the security department do your new joiners have now?

You may also be interested in how the security messages have translated into the development of an appropriate security mind-set and behaviours in the workplace. You could ask new joiners:

- How have they been able to apply what they have learnt with the security messages in the workplace?
- Were there any gaps in what was learnt in the security messages programme that they needed in order to behave securely in the workplace?
- Were they able to access the relevant security information from other sources as and when required?

Line managers and/or those in security 'champion' type roles may be able to support you in building this picture of how well new joiners have applied what they have learnt back in the workplace.

When conducting a survey you should aim to reach as many new joiners as possible, across a range of departments/teams/roles and demographic characteristics (e.g. age, gender, grade/seniority). This will ensure you have a representative sample of your workforce when drawing conclusions about the impact of your security messages for new joiners.

You may have other sources of data to support you in the evaluation of the campaign. Speak to your IT monitoring team, physical security team, and/or HR for further ideas on what additional data might be available to you.

You will have a good idea of the measures of success that are specific to your organisation. Overall, if the net result is that new joiners engage with security from the outset, develop an appropriate security mind-set and are aware of what they need to do to keep the organisation secure, then you can be confident that your security messages programme has been successful.

Revisit your security messaging over time to ensure that it stays up-to-date and relevant based on the threats you face and changes to the operating environment and working practices.

05

Supporting resources

CPNI supporting resources

CPNI has a range of resources that you may find useful in educating new joiners and influencing their mind-set and approach to security. These can provide a head-start in developing your security messages, particularly if you're stretched for resources. Many of the resources include editable materials and have been designed specifically to be appealing to employees.

Please contact CPNI to update us on your use of these materials and the impact they have had in your organisation. Check the CPNI website or with your CPNI adviser for details of any new campaigns and resources.

Social engineering campaign

This campaign educates employees by raising awareness about what social engineering is, what an approach might look like, and how employees can better protect themselves against this type of threat. The campaign kit includes: how to run the campaign, a briefing guide, quiz, checklists, posters and video.

It's OK to say campaign

This campaign has been designed to help employees identify behaviours in the workplace that strike them as unusual or concerning and to encourage them to take appropriate action, rather than just 'shrugging' them off.

The campaign is centred around the 'It's OK to say' animated film, which presents the unusual behaviours in a light-hearted way. Materials also include a 'How to' guide for organisations, posters and pocket-sized cards.

Digital footprint campaign

This campaign is designed to help employees understand what their digital footprint looks like, how to manage and monitor it, and what impact it could have on them, their colleagues and their organisation if they fail to do so. The campaign kit includes: advice on how to run a digital footprint campaign, eight posters and two booklets for employees with resources to help them to actively manage their digital footprint.

Line manager campaign

Line managers have a key role to play in embedding behaviour change within an organisation. To help encourage greater ownership and responsibility for security, CPNI has developed practical advice to help managers brief their team on security.

The campaign kit includes advice for line managers on how to promote security in the workplace, a checklist of security issues to remember, stickers that can be issued to employees and a video for line managers.

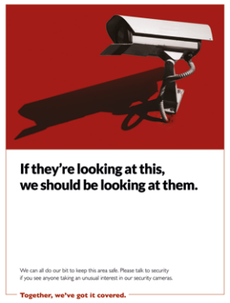
Small actions, big consequences: your guide to being security savvy

As signposted in the 'What new joiners need to know and do to be secure' section of this guidance. CPNI has developed two products to provide examples of effective and less effective employee security behaviour at work, outside of work and online. One product is 'A framework for CNI organisations on security savvy employee behaviour' aimed at security managers (and others internally) to guide design of internal security policies and practices. The second is a booklet for CNI employees to educate and raise awareness of what good security practice looks like.

Employee vigilance campaign

How employees behave is a key indicator of an organisation's attitude to security. Vigilant security behaviour – such as showing awareness of one's surroundings or engaging with strangers – will show anyone with hostile intent that they have more to worry about than just security guards and CCTV.

CPNI has developed this campaign to help organisations instil vigilance behaviours in their employees. The campaign kit includes advice on how to run an employee vigilance campaign, posters, a wallet card and personal security advice for employees.



Workplace behaviours campaign

This campaign kit has been designed to help individual staff members ensure that they are getting the security basics right in and around the workplace. It addresses seven basic behaviours (e.g. locking unattended IT devices, secure destruction of sensitive information and escorting visitors).

The campaign kit includes advice on how to run a workplace behaviours campaign, a briefing guide and quiz, stickers, posters, a video and checklists for employees.

- ## CPNI personnel security animations

  1-2 min films available on the CPNI website and CPNI YouTube channel **(https://www.youtube.com/user/UKCPNI)**

- ## Your company needs you – who's responsible for security?

  A general induction to security. It highlights some common physical, IT and personnel security weaknesses.

- ## People, people, people – you are your company's greatest asset

  Based on the true story of a diamond thief who used social engineering to undermine physical security measures.

- ## Fly in the ointment – management responsibility for employee risk

  Managers are responsible for security issues, should lead by example and take necessary action.

- ## You choose – effective management

  Good managers intervene before an insider act can occur.

- ## One small step – security measures needn't cost the earth

  This film shows managers that small changes to culture can significantly improve the effectiveness of existing security measures.