CPNI

Centre for the Protection of National Infrastructure

Embedding Security Behaviours: using the 5Es

A framework for improving security behaviour within organisations

Contents

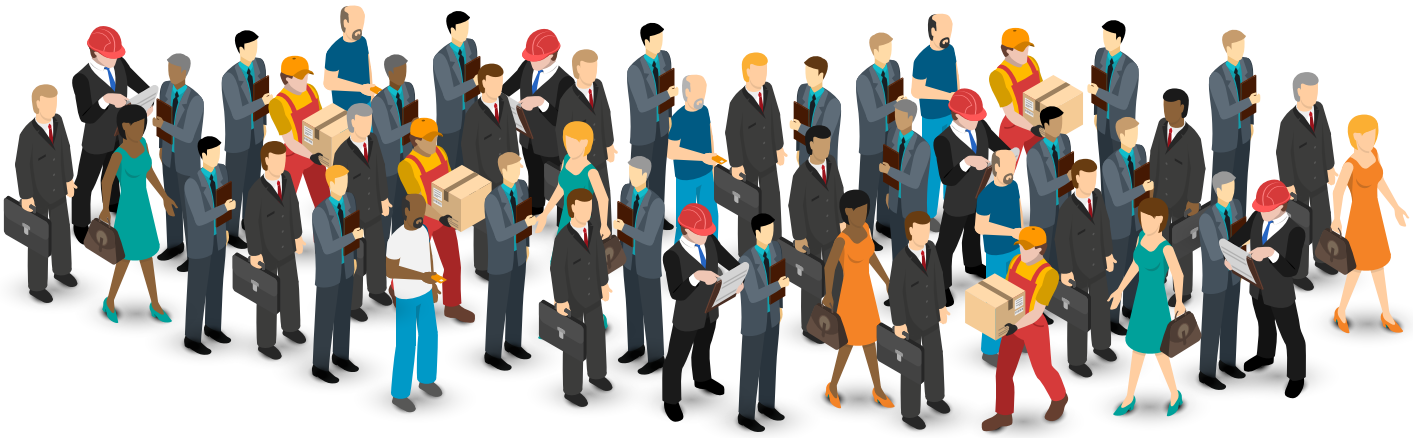
Overview

This document is designed for those responsible for **developing and sustaining effective security behaviours** within a Critical National Infrastructure organisation.

Employee security behaviour is central to protecting UK Critical National Infrastructure from terrorism, espionage and other threats. The development of an **appropriate security culture** within UK organisations, where the right **security behaviours** are adopted by the workforce as a matter of course, is an essential component to any protective security regime. It is also something that can be achieved at a relatively low cost in comparison to some physical and technical measures.

Following five years of research into security culture and security behaviour, CPNI has developed a simple, comprehensive yet **practical framework** for how to embed security behaviours and create an environment that sustains these within organisations. This framework is called the **5Es**. The framework draws on current academic thinking in behaviour change, change management, and influence as well as learning through CPNI's practical experience in security culture programmes.

"Five years of research helped to shape this framework."



The role of people in protective security

An effective protective security regime relies on the successful coordination and integration of **physical, cyber** and **people** related security measures to keep critical assets secure.

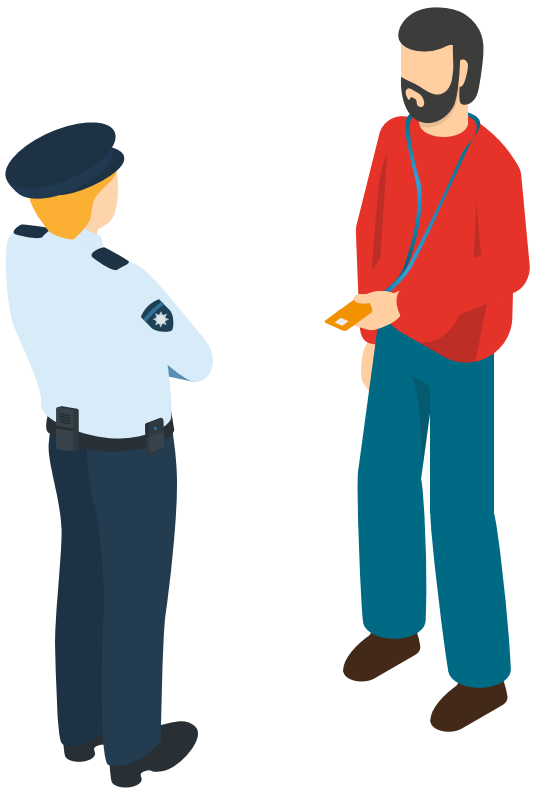
Physical and cyber (or information) security measures can only go so far in mitigating security threats. **Employees** must behave in the right way to optimise the effectiveness of such measures. In addition, employees can act as a protective measure in their own right, playing a significant role in the detection, deterrence and prevention of potential security threats (See CPNI OFFICIAL level documentation on 'Hostile Reconnaissance'1, 'Employee Vigilance Behaviour Campaign'2, and 'Insider Data Collection Study'[3]).

Whilst we may recognise the **vital role that people can play** in protective security, marshalling employees to be security conscious, and establishing a work environment that sustains this, can be challenging. The 5Es framework is designed to support organisations with this.

Precisely what influences behaviour remains the subject of debate amongst psychologists, sociologists, anthropologists, economists and others alike, but it is agreed that it is the product of a multitude of **interrelated factors**. Consequently there is not a standard solution.

> "Employees can act as a protective measure in their own right"

The approach that will work best for one organisation is likely to be different for another as it will be dependent on context. However there are some key principles, evidenced by the **latest research and thinking**, that can ensure an organisation has the right combination of interventions in place to encourage employees to play their part in the protective security picture.



[1] http://www.cpni.gov.uk/advice/Personnel-security1/Hostile-Reconnaissance-Understanding-and-countering-the-threat/

[2] http://www.cpni.gov.uk/advice/Personnel-security1/Employee-vigilance/

[3] http://www.cpni.gov.uk/documents/publications/2013/2013003-insider_data_collection_study.pdf?epslanguage=en-gb

Using the 5Es framework

Before utilising the framework, it is crucial that an organisation is clear on the security behaviours it desires from its employees.

This means considering the following:

- What assets require protection?
- What security threats are currently facing the organisation?
- What level of security risk is the organisation exposed to?
- What is the organisation's security risk appetite?
- What level of protective security is proportionate?

CPNI can provide guidance on a number of these areas. For example, information on current security threats, risk assessment methodology, risk management practices and implementing proportionate security mitigations is available on our public website at www.cpni.gov.uk, our extranet (OFFICIAL SENSITIVE) and on the NCSC (National Cyber Security Centre) website.

Once an organisation has considered these factors it will be in a more informed position to decide on the security behaviours it would like its employees to undertake that complement existing physical, cyber and personnel measures.

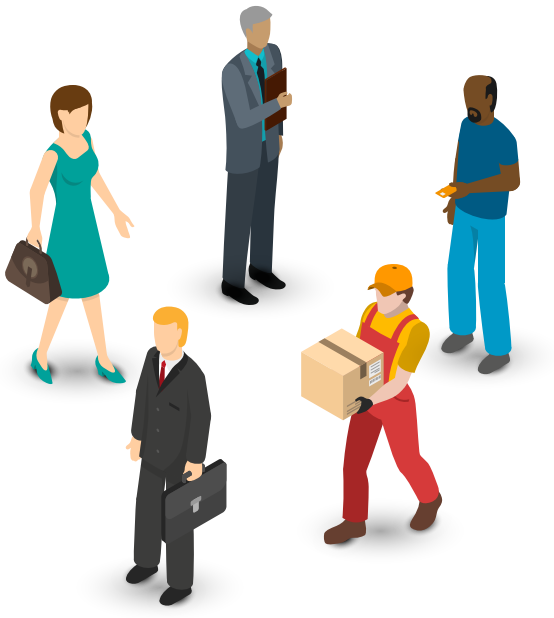
Consideration of these factors will also assist the organisation with determining how it would like to manage and approach security from a strategic perspective, thereby shaping its security culture.

It is at this point that the 5Es are best utilised to help embed the desired security behaviours and culture in the everyday working practices of employees.

Please note, this framework does not endorse an approach to protective security whereby employee behaviour is considered as an afterthought once the physical, cyber and/or personnel security measures have been put in place. Good practice dictates that all security measures should take employee behaviour into account and should not be designed in isolation from the user. The 5Es framework supports this – under the E of 'Shaping the Environment' – and advocates the importance of taking a people-centred approach to protective security.

However, it is worth noting that the design of physical and cyber security practices that consider user behaviour can be a specialist area that professionals such as behaviour change and human factors experts can assist with, and readers are advised to consider this accordingly.

"All security measures should take employee behaviour into account"



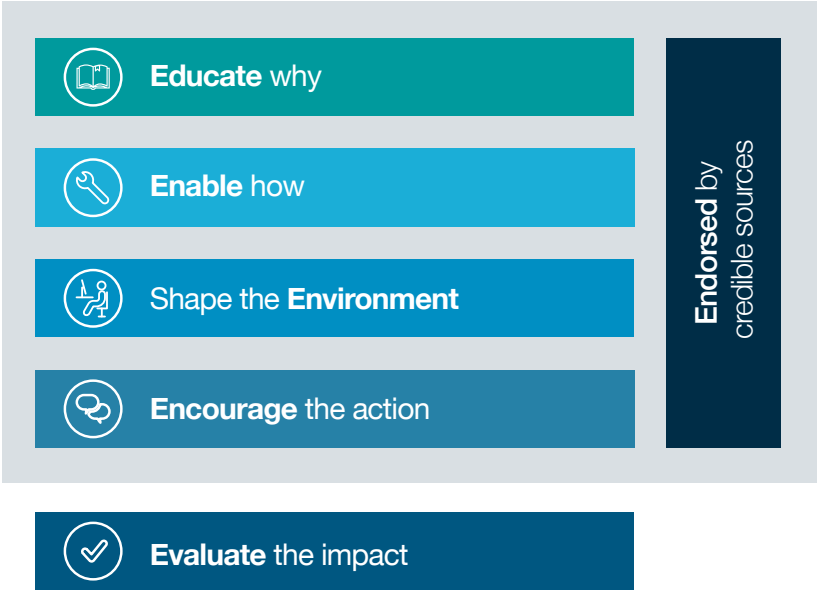
Introducing the 5Es

Once an organisation is clear on the role it would like its people to play in protective security, the **5Es** provides a framework to guide organisations on how best to **embed and sustain** these behaviours within the workforce.

The framework has been **developed by CPNI**, in conjunction with leading academics and experts in the fields of behaviour change and organisational change. It primarily draws on Protection Motivation Theory[4], the COM-B model[5] of behaviour change, and influence research (e.g. Cialdini, 2007[6]) as well as CPNI experience in the practical application of security behaviour programmes. However other research studies also offer support for the framework (e.g. Williams, Harkins & Latane, 1981[7]; George, 1992[8]).

The framework can be applied to behaviours within the physical environment (e.g. an office or site) and those within the digital environment (e.g. email or social media). It relates to behaviours associated with tasks (such as pass wearing, locking computers, and escorting visitors) and style (such as accepting and complying with the policies, or questioning and adapting security practices to something that better suits the needs of the individual).

The 5Es framework



The framework illustrates that when any of these principles are not in place, the likelihood of successfully achieving the desired behaviour is diminished. The five principles are supported by a sixth element – **Endorsed by credible sources**. This proposes that the impact of four of the Es (the first four listed) can be augmented by the presence of credible sources who visibly endorse these messages (e.g. Head of Security, CEO, Board members, senior management). A detailed description of each of the principles within the framework is provided in the next section 'Explaining the 5Es'. A summary of the framework and the key points to take away are presented in appendix 1.

[4] Rogers, R. W. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In J. Cacioppo & R. Petty (Eds.), Social Psychophysiology. New York, USA: Guilford Press.

[5] Michie, S., van Stralen, M.M. & West, R. (2011). The behaviour change wheel: a new method for characterising and designing behaviour change interventions. Implentation Science, 6:42.

[6] Cialdini, R. B. (2007). Influence: the psychology of persuasion. New York, Collins

[7] Williams,K., Harkins, S., & Latane, B. (1981). Identifiability as a Deterrent to Social Loafing: Two Cheering Experiments. Journal of Personality and Social Psychology, 40(2), 303-311.

[8] George, J. M. 1992. Extrinsic and intrinsic origins of perceived social loafing in organisations. Academy of Management Journal, 35: 191-202.

Explaining the 5Es

A detailed description of what each of the principles within the framework is about is provided in this section, alongside guidance on how this can be achieved within an organisation and example interventions that can be used.

Educate why

What is this about?

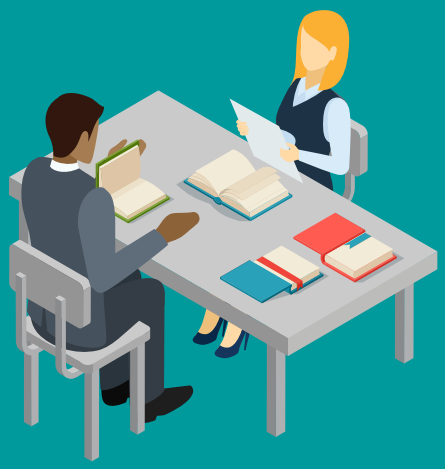
Educating employees about the security threat. Employees are less likely to adopt the required behaviours when they are uninformed of the susceptibility to threats (both their own and the organisation's susceptibility) and the severity of the consequences.

How can this be achieved?

- **Educate employees on their susceptibility to security threats given where they work** e.g. What threat actors are interested in the organisation and its employees? How might, or do, they target the organisation? What assets are they most interested in?
- **Educate employees on why these threats matter to the organisation** e.g. How do they impact on the organisation's ability to deliver its core work? What harmful implications are there to services, customers, employees or business reputation?
- **Educate employees on the benefits to them of demonstrating the security behaviours** e.g. What are the positive benefits in relation to their role? What are the possible negative consequences or penalties for them if they do not adopt the behaviours? What benefits apply outside of work such as to their personal life or family?

Example interventions

- Threat updates
- Case-studies
- Intranet articles
- Interactive security events
- Management briefings
- Aligning security to core business goals
- Role profiles or job descriptions
- Performance appraisals



Enable how

What is this about?

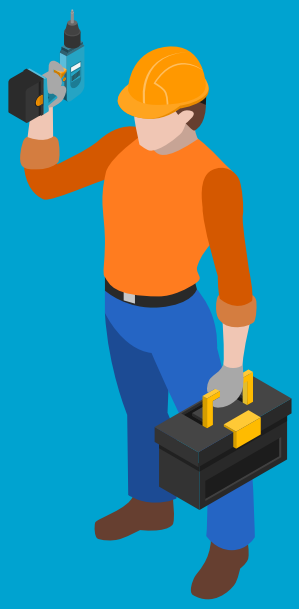
Enabling employees to demonstrate the behaviours being asked of them. If employees aren't provided with the appropriate information, training, advice and support they may not know what security behaviours are expected of them, how to do these, or have the necessary confidence to demonstrate them.

How can this be achieved?

- **Explain to employees what security behaviours are expected of them** e.g. What does good security behaviour look like? What does poor security behaviour look like? What security behaviours are expected in different roles, buildings or work areas?
- **Equip employees with the knowledge and skills so they feel capable and confident in demonstrating the security behaviours** e.g. What do employees need to know to be able to perform the behaviours? What skills do they need to have? Are all employees confident in enacting the behaviours or does it vary by demographics, roles or business areas?

Example interventions

- Security behaviour hand-outs or booklets
- Annual security refresher training
- Role-specific security training
- Security events
- 1:1 mentoring or buddying
- E-learning
- Knowledge checks
- Role profiles or job descriptions



Shape the Environment

What is this about?

Shaping the environment to enable employees to demonstrate the desired security behaviours easily. This is about ensuring that employees have the resources they need (e.g. equipment, materials, people), the physical opportunity (e.g. space, time, access) and the social opportunity (e.g. peer pressure, leadership, support) to demonstrate the behaviours. If employees perceive that there are too many hurdles or barriers to applying the behaviours in a practical setting, they will be less likely to do so.

How can this be achieved?

- **A physical work environment where security behaviours are easy to do** e.g. Are security processes and procedures simple to follow? Is security related information easy to find and digest? Do employees have the tools and equipment needed? Are the systems, processes and technology making security easy or cumbersome? Is there sufficient time in the day for security? Are there prompts and reminders to help?

- **A social environment where doing security the right way is valued, respected and seen as the norm** e.g. Do managers lead by example? Do peers support one another with security tasks? Will employees challenge one another on poor security? Do organisational processes, systems and activities promote and reinforce good security practice?

Example interventions

- Redesign of security policies
- Redesign of IT systems
- Performance appraisals
- Induction activities
- Training activities
- Reporting processes
- Leadership briefings
- Managers leading by example
- Workplace equipment
- Posters
- Reminders

Encourage the action

What is this about?

Providing feedback to employees to encourage the desired action and discourage the undesired action. This is absolutely key to sustaining security behaviours in the workplace. If employees receive little or no feedback when trying a new behaviour, or they associate the behaviour with a negative experience, they may be less likely to perform the behaviour again. This can mean that any observed improvement in security behaviour is short lived and will subside over time.

How can this be achieved?

- **Provide employees with feedback on their security behaviours** e.g. Is feedback on security behaviour provided during performance appraisals and team meetings? Are employees encouraged to learn from their own and others' security actions? Are corporate communications used to report on and praise good security practice and address poor performance or mistakes? This E links closely back into the E for Educate why.

- **Provide tangible and/or intangible incentives** e.g. Are employees thanked for reporting a security concern or incident? Is recognition provided by management for positive security behaviour? Are there rewards or career benefits for adhering to good security practice? Are there consequences and sanctions built into systems for employees who don't comply with important security policies and practices? Is poor security behaviour visibly challenged and managed?

Example interventions

- Breach policies

- Soft and hard incentive schemes or programmes

- Acknowledgement and thank you messages

- Publishing blogs and articles on positive and negative security stories

- Corporate communications on the organisation's security performance

- Intranet articles and case-studies on how staff behaviour is impacting on the threat

Evaluate the impact

What is this about?

Evaluating the impact that the interventions have on employee security behaviour. Organisations should assess the extent to which the time, resources and costs involved have had a positive effect on protective security, and whether improvements or modifications in the approach are required. Any lessons that have been learned must then result in effective action so staff can see these have been made. This will help to ensure that future behaviour change activities remain current and valid, and that any changes in contextual factors are considered.

How can this be achieved?

A simple evaluation may involve sense checking that the activities and interventions are having an impact through a short survey with staff (e.g. online or face-to-face). A more comprehensive evaluation may involve taking pre- and post measures over 18-24 months against a range of metrics through multiple data sources. Whichever approach is taken, organisations should aim to do the following:

- **Identify key performance indicators (KPIs) or measures of success against which to evaluate progress.** What are the aims and objectives of the intervention? What outcomes are expected in the short, medium and long term? What changes in knowledge, attitudes and/or behaviours will there be? Could there be additional consequences you haven't anticipated that you should measure?

- **Consider ways to assess metrics, preferably over time**. What quantitative measures are available such as breach records, reports of suspicious activity, observational data or survey data? What qualitative measures can be collated through focus groups, interviews or open survey questions? Can measures be taken pre- and post interventions to show the scale of change?

CPNI has further tools and guidance that can assist organisations with evaluation. For example, 'Has it worked? An evaluation guide for an internal security behaviour campaign' and the CPNI Security Culture Survey Tool (suite of surveys to assess behavioural and cultural change).

Example interventions

- Staff surveys

- Intercept surveys

- Focus groups

- IT monitoring

- Breach records

- Observation studies

- CPNI security culture survey tool

The role of endorsement

Finally, the effect of the first four Es will be augmented if they are perceived by the workforce to be endorsed by credible sources. These credible sources may be external to the organisation (e.g. security experts, police, CPNI, ex-cyber-hacker) or internal to the organisation (e.g. Head of Security, Head of IT, CEO, the Board).

Therefore it is paramount that, when designing interventions around the 5Es, an organisation considers who will be the 'messenger' of the interventions (e.g. who will be the voice of the campaign or change programme? Who can make the messages really resonate with employees?)

Key things to remember when endorsing a message or change are:

- Different groups of employees may need endorsement from different people (e.g. for new employees the message may be best delivered on induction by the Head of Security, whereas for existing employees who may be cynical about the change the message may be best delivered by an external credible source who can clearly articulate why something is a threat and what action employees should take).
- The personal touch can also help to make the messages meaningful and impactful to employees (e.g. the Head of Security being quoted through internal communications to say how much they value a report-in from employees in relation to unusual or suspicious behaviour around a site, and what the Head of Security has done to action the report).
- The message must always be seen to be endorsed consistently from the top of the organisation. Examples of ways in which leaders can do this include statements of endorsement in educational materials, attendance and visibility at events, inclusion in senior level communications to staff (e.g. briefings, newsletters), engaging in formal and informal conversations around the behaviours.

Implementing the 5Es

The 5Es provides a useful framework to follow for embedding security behaviours and creating an environment that sustains these.

It is advisable to have the following in place to maximise its impact:

- **Data on the current status** – organisations should have a measure of where they are now in relation to the security behaviours they wish to embed.

  For example: How frequently are employees demonstrating the desired behaviours today? What are the primary factors or reasons behind why this may or may not be happening (e.g. is it lack of understanding, lack of motivation, lack of the right equipment or resources, poor design or the workplace?) This will help with knowing how big the proposed change is, and where the priority areas for intervention may lie (e.g. should there be a greater focus on 'Shaping the Environment' or 'Educating Why'?).

- **A project team** – it is important that there is a sufficiently resourced project team available to lead and coordinate the roll-out of the programme. This is key to ensuring timely messages are communicated across the organisation as well as coordinating activities and providing clear lines of accountability.

  It is advised that the project team consists of representatives from the security department, HR team, and communications team as well as representatives from the organisation (e.g. security champions) who can help to design the programme. Appendix 3 details the APEASE criteria which can be a useful framework to guide the design of practical interventions.

- **Communications strategy and message** – the development of an overarching security culture message and supporting communications strategy can help to augment the impact of your programme (e.g. "Together we've got security covered" or "Helpful vigilance").

  A consistent message to underpin the programme will help it to become easily recognisable. However it is important that this is in keeping with the wider culture of the organisation so that it is perceived as being aligned and complementary to other workplace initiatives.

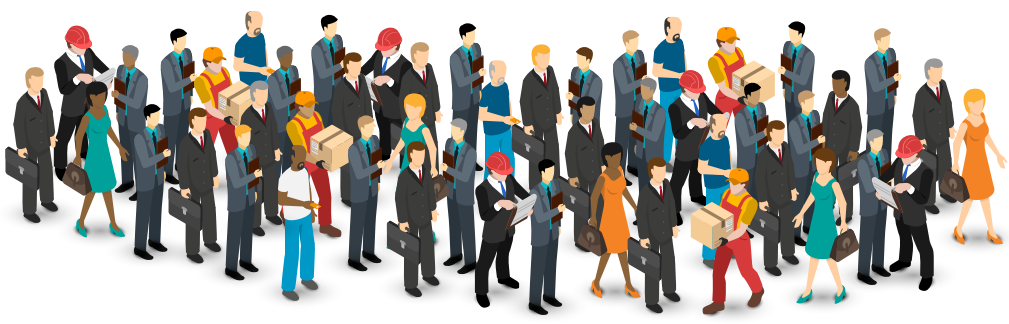
- **Senior management and Board level support** – this will be important, not only in terms of securing top level endorsement for the programme overall, but for enabling any changes to policies or processes to be approved in a timely manner. If senior level support cannot be achieved upfront, then a senior level sponsor will be required who can take the lead on briefing seniors on the work and any decisions that are needed.

Taking an integrated approach

Whilst the 5Es have been presented in this document sequentially, they will be most effective if they are integrated with one another in an iterative way. This is because an organisation's ability to flex between the principles will be important as requirements change. For example, there may be times when a focus on 'Educating why' is the priority whereas at other times 'Enabling how' may be key.

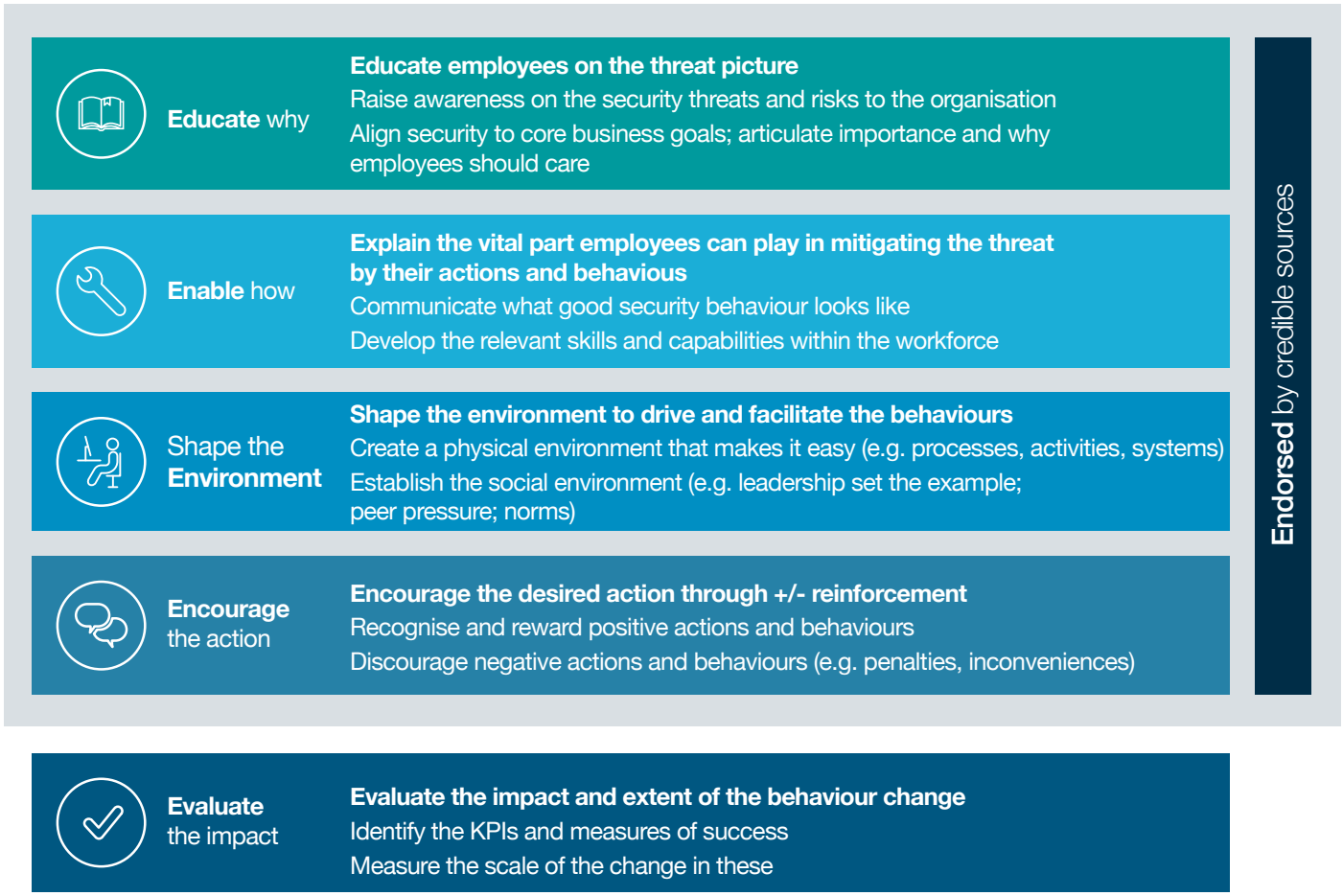
Finally, when implementing the 5Es, please bear in mind that there is a limit as to how much information employees can take on board at any one time. Whilst an organisation may identify a number of areas where significant strides in employee security behaviour is required, it is advisable that this is tackled in a step by step fashion. Identifying 3-4 priority behaviours for change in Year One may be a helpful starting point on which to build, as you move into Years Two and Three of the programme.

The 5Es model will continue to be reviewed and evaluated by CPNI. As we update our research, we will make updates to this guidance and our corresponding products accordingly.



Appendix 1:

5Es to embedding security behaviour



Appendix 2:

Worked example of the application of the 5Es

An organisation identified that it needed its workforce to adopt vigilant, security savvy behaviours when entering and leaving their secure site. There were a number of reasons for this such as:

a) the organisation's security guards were not able to be everywhere all of the time and so staff could assist with spotting unusual or suspicious behaviour;

b) staff were often best placed to pick up on things that stood out from the ordinary;

c) hostile reconnaissance research had shown that vigilant staff behaviour could act as a deterrence to those planning an attack;

d) staff would be more alert to potential threats if they were alert, rather than distracted, when entering or leaving the site;

e) staff were making the site and themselves vulnerable by wearing their passes in local shops, meaning it was easier for hostile attackers to identify workers and/or learn what the identity badges looked like.

How the organisation applied the 5Es framework

Educate why

To educate staff on why being vigilant mattered when entering and leaving the site, and to build motivation for adopting the desired behaviours, the organisation carried out the following activities:

- Reminded staff that the site housed sensitive information that others (e.g. protest groups, organised criminals and some hostile foreign states) were interested in acquiring which made the site, and its staff, an attractive target for attack.
- Provided examples from their site (and similar sites in the UK) where suspicious activity had been observed or had taken place and how the behaviours of staff (e.g. pass wearing outside, lack of reporting of suspicious behaviour) had aided the potential attacker.
- Provided senior managers with a tailored and more detailed briefing on the threat to emphasise the business reasons for taking protective security seriously.
- Demonstrated the link between the compromise of sensitive assets and the organisation's ability to deliver essential services to its customers, having a knock-on implication for business reputation, revenue and future growth, as well as causing distress to customers.

The organisation communicated these messages through internal communications (e.g. newsletters) and departmental face-to-face briefings.

Enable how

So that staff were not overly alarmed, it was critical that the organisation provided appropriate information, training and support on (a) the existing security measures that were in place, and (b) the critical role that staff could play to strengthen these existing measures and to help keep them and the organisation secure. The organisation did this by carrying out the following activities:

- Reassuring staff that particular protective security measures were in place and demonstrating this where possible (e.g. security control room open days to demonstrate the state of the art CCTV; reinforcing that there was a highly competent security team).
- Briefing staff on the key behaviours that they should adopt when entering or leaving the site (e.g. to be alert and vigilant when entering and leaving the site rather than be distracted by mobile phones or music devices etc.; to report anything unusual or suspicious immediately to security by following the correct process; to follow the correct entry and exit procedures for passing through gates and vehicle barriers to prevent unauthorised access; to put on their security pass as they enter the building and remove it as they leave).
- Producing cartoon strips that illustrated the behaviours, so the workforce could see examples of these in action.
- Providing staff with the telephone number to call, if they saw something unusual or suspicious, on a handy wallet card so they knew what the reporting number was and that this was easily accessible.
- Reissuing all the entry and exit procedures (for gates and vehicle barriers), making sure these were simple to follow and clear so that staff (and security guards and receptionists) had a shared understanding of what these were.

The organisation communicated these messages through internal communications (e.g. newsletters) and departmental face-to-face briefings as part of their communications strategy.

Shape the Environment

The organisation recognised that educating staff on what the threat was, and then enabling them to demonstrate the security savvy behaviours, would not be enough to achieve the desired goal. They therefore looked at the physical and social environment (i.e. the context) in which the behaviours would be demonstrated and then carried out the following activities:

- In relation to the physical environment, the organisation identified that there was very little in or around the entry and exit points to prompt staff to be vigilant or to wear their pass inside and to remove it when they leave. They therefore developed some eye-catching posters and images to remind staff to demonstrate these behaviours, and positioned these in appropriate, helpful places.
- To make it easier for staff to follow the correct entry and exit procedures (rather than allow tailgating which was happening from time to time) the organisation recognised that it would need to redesign one of the reception areas so that there were sufficient numbers of swipe enabled speed gates. This work was subsequently carried out.
- To instil the right culture and attitudes towards security, the organisation redesigned some of its corporate processes, systems and activities, such as the induction process and annual security training, to ensure the importance of good security practice (and specifically, employee vigilance when entering and leaving sites) featured prominently in these.
- The organisation provided a brief to senior managers to reiterate the important role they had in leading by example, such as pass wearing on site.

Encourage the action

To sustain the vigilant behaviours and embed them in the 'norm' of the workforce, the organisation considered what it could do to recognise and reinforce the actions of those who demonstrated the desired behaviours, and encourage those who weren't adopting the behaviours to do so. The activities they conducted included the following:

- Ensuring that every member of staff who reported unusual or suspicious activity received a thank you and an acknowledgement from the Head of Security so that they knew their report had been received and was being taken seriously.
- Ensuring every staff report was recorded and periodically, every three months, the organisation published an article on its intranet updating staff on the number of reports received, thereby providing a high-level overview of suspicious activity and action taken. This helped to recognise the good practice of those staff members who were reporting genuine concerns, as well as educate other staff members on the types of suspicious activity the organisation would welcome hearing more about.
- Giving the security guards permission to immediately challenge (in a friendly manner) those who entered or left the site without following the correct procedures and/or were using mobile phones or music devices (an indicator of poor situational awareness). The guards did this by stopping the individual(s) concerned and handing out an A5 card that reminded them of the importance of being vigilant (in relation to the threat) and reiterated the good security behaviours required. After six months, once the behaviours had been embedded, the organisation introduced a new breach policy for anyone who was caught tailgating through the gates or who wasn't wearing their pass on site.

Endorsed by credible sources

The organisation recognised that a critical way to embed the behaviours in the organisation was to show that they were fully supported and endorsed by those that the workforce were likely to respect and perceive as credible. Therefore the organisation did two things:

1. They invited an external speaker, who was an expert in conducting hostile reconnaissance, to come into their organisation to brief staff on how hostiles typically plan physical attacks of sites (like the organisation's) and why the behaviour of the staff has an impact on their ability and confidence in being successful. This was videoed and put on the security pages of the organisation's intranet for those who couldn't attend the session to view at their convenience.
2. The Head of Security and the CEO of the organisation were both very vocal in providing their support and backing to the importance of the behaviours in relation to protective security. This took the form of a newsletter by the Head of Security on the organisation's intranet (featuring on the main page) and a two-minute brief on the campaign by the CEO as part of her quarterly talks to staff. Finally, all line managers were provided with a short brief to deliver to their staff, as part of their regular team meetings, on the importance of staff playing a part in protective security.

Evaluate the impact

Prior to launching the programme to embed the new behaviours, the organisation was already recording some metrics that could be used to assess the extent to which staff were demonstrating the behaviours. For example, they recorded the number of reports made by staff regarding unusual or suspicious activity around the site. They also had anecdotal feedback from the security guards regarding percentages of staff wearing passes on site/off site and incidents of tailgating, although this data wasn't particularly scientific.

In order to identify additional useful metrics, the organisation developed some key performance indications (KPIs, or measures of success). These were as follows:

a) for 90% of staff to demonstrate vigilant security behaviours when entering and leaving the site;

b) for staff to feel comfortable and willing to report any unusual or suspicious behaviour to security that they might observe around the site;

c) for 100% of staff to use the correct entry and exit procedures onto the site;

d) for 90% of staff to wear their security pass onsite and to remove this every time they left.

The organisation then undertook an evaluation study to gauge where the organisation was (in relation to these KPIs) prior to launching the programme. They did this by observing a sample of staff for one hour, twice a day for three days, in relation to their pass wearing activity and vigilance behaviour. They also stopped 60 staff and asked them to complete a short seven item questionnaire regarding their knowledge of and attitude towards the desired security behaviours.

These results indicated the organisation was a long way away from reaching its KPIs. Following the launch of the programme, the organisation reran the evaluation study two weeks later and then three months later to measure progress and to gather feedback on whether the approach was resonating and having the desired effect. Substantial improvements had been made in relation to the KPIs, however staff feedback highlighted that some additional interventions needed to be put in place for the security guards and for some line managers in order that the approach continued to engage (rather than demotivate) staff.

30%

more staff were wearing their passes onsite and taking them off when leaving, and security had seen a

four-fold increase

in high quality staff reports of unusual or suspicious behaviour

The organisation plans to evaluate the impact of the programme again in 12 months' time. The feedback from this will inform how best to shape the 5Es model for the following year.

Appendix 3:

APEASE Criteria

The APEASE criteria[9] for designing and evaluating interventions:

Criterion	Description
Affordability	Interventions often have an implicit or explicit budget. It does not matter how effective, or even cost-effective it may be if it cannot be afforded. An intervention is affordable if within an acceptable budget it can be delivered to, or accessed by, all those for whom it would be relevant or of benefit.
Practicability	An intervention is practicable to the extent that it can be delivered as designed through the means intended to the target population. For example, an intervention may be effective when delivered by highly selected and trained staff and extensive resources but in routine clinical practice this may not be achievable.
Effectiveness and cost-effectiveness	Effectiveness refers to the effect size of the intervention in relation to the desired objectives in a real world context. It is distinct from efficacy which refers to the effect size of the intervention when delivered under optimal conditions in comparative evaluations. Cost-effectiveness refers to the ratio of effect (in a way that has to be defined, and taking account of differences in timescale between intervention delivery and intervention effect) to cost. If two interventions are equally effective then clearly the most cost-effective should be chosen. If one is more effective but less cost-effective than another, other issues such as affordability, come to the forefront of the decision making process.
Acceptability	Acceptability refers to the extent to which an intervention is judged to be appropriate by relevant stakeholders (public, professional and political). Acceptability may differ for different stakeholders. For example, the general public may favour an intervention that restricts marketing of alcohol or tobacco but politicians considering legislation on this may take a different view. Interventions that appear to limit agency on the part of the target group are often only considered acceptable for more serious problems.
Side-effects/safety	An intervention may be effective and practicable, but have unwanted side-effects or unintended consequences. These need to be considered when deciding whether or not to proceed.
Equity	An important consideration is the extent to which an intervention may reduce or increase the disparities in standard of living, wellbeing or health between different sectors of society.

[9] Michie S, Atkins L, & West R. (2014). The Behaviour Change Wheel: A Guide to Designing Interventions. London: Silverback Publishing.