CPNI
Centre for the Protection of National Infrastructure

**Security Culture**

PUBLISH DATE: January 2022

CLASSIFICATION: Official

# An Introduction to Security Culture


## Executive summary:

- People form a vital part of any successful protective security measure.
- People can do more than Prevent security incidents, they can also actively Detect and Deter security threats.
- To harness the POWER OF PEOPLE in your security defences, you need people to actively demonstrate security savvy behaviours AND have a working environment that informs, encourages and supports them to do this. This takes time, work and resources.
- Developing a strong and appropriate security culture is one approach to achieving this. A way to achieve this is by identifying and strengthening high priority security behaviours, and gradually build on these changes.
- Adopting CPNI's "5Es to embedding security behaviours" presents a practical and cost-effective approach for improving security behaviour, that also aims to strengthen your security culture over time.
- To help you on your way, CPNI has a range of off-the-shelf campaigns ready to use right now, alongside other supporting guidance.
- This document provides an overview of security culture for any organisation who own valuable assets, be that physical property, knowledge and information, people or public spaces, that require protection.


1. Any site or organisation can be vulnerable to security incidents when people do not act in a security conscious way.

2. People include an organisation's employees, contractors and suppliers, but also its visitors and ex-employees (such as those who have been dismissed, retired, or moved on to work elsewhere, who may still hold sensitive access, information or knowledge).

3. People can do more than **Prevent** security incidents. They can actively **Detect** and **Deter** security threats. Therefore, people form a vital part of any successful protective security measure, alongside appropriate physical and cyber security measures.

4. **How do people help?** Through the demonstration of effective security behaviours BUT WITH the support of an organisational culture that is alive with systems, procedures, messaging, and activities that value and enable security minded action (i.e. an appropriate security culture).

5. **What is an appropriate culture?** The precise nature is unique to each organisation as it depends on factors such as the sector the organisation operates in, what its core mission is, what security threats it faces, and the consequences to business, staff, customers and/or the public, should a security incident take place. While there is no one-size-fits-all, there are some common elements we would expect to see in organisations. For example:

    a. Employees know why security matters to the organisation, such as the threats their organisation faces, and the consequences should an incident occur.

    b. Employees know what is expected of them in relation to security, and how to do this. By this we mean that desired attitudes and behaviours are clearly defined, and that information on what to do and how to do it is clearly communicated and shared with employees.

    c. The organisational systems, processes and activities that shape behaviour are designed to "help" rather than hinder the desired security behaviours and attitudes. For example, the induction, training, management support, reward and breach systems and the working environment help embed the desired behaviours and attitudes, rather than contradict or undervalue them.

    d. Employees take responsibility for doing security well. They understand that the responsibility for security is shared by everyone in an organisation, and not taken care of by individuals, or physical or cyber security measures alone. They are clear on the part they play in keeping the organisation secure.

6. As a result of having an appropriate culture in place, an organisation may see the following type of outcomes and measures of success:

    a. A workforce that are engaged with and take responsibility for security issues
    b. Increased compliance with protective security measures (e.g. reduced breaches)
    c. Reduced risk of Insider Incidents
    d. Awareness of the most relevant security threats
    e. Evidence of employees thinking and acting in a security conscious manner (e.g. reporting near misses, reporting mistakes and errors, reporting concerns about employees, suggesting improvements to current security processes and systems)

7. We cannot expect people to automatically know what good security behaviour looks like, or to naturally do this, given work pressures and time constraints experienced. Today's security threats are complex, and organisations are busy and dynamic places. People need help and support to understand what the security threats are and to be guided on making the right judgements and decisions at the right time when it comes to security. This needs to be maintained over time, as security threats evolve and the organisation changes.

8. This means a programme of security education is key. All managers, leaders and security professionals have a pivotal role to play in security education and developing effective security behaviours in people. CPNI recommends adopting our "**5Es to embedding security behaviours"** approach to doing this. This involves:

    a. ***Educating*** **people on what the security threats are today** (for example, who the threat actors are, what they are interested in, how they might target the organisation, the consequences if they were to succeed, and the benefits of stopping them to limit harm to employees, the business and the public)
    b. ***Enabling*** **them to demonstrate security savvy actions** (for example, explaining to people what they can do to protect sensitive assets, and equipping them with knowledge and skills so that they feel capable and confident in doing so)
    c. **Shaping the *Environment* to support people in being able to demonstrate these behaviours easily** (for example, creating a physical environment that prompts people on the good practices to use, and makes these simple, practical and easy to do whether it be in a building, working online, or operating some important equipment. It also involves creating a social environment where doing security the right way is seen as valued, respected and the norm)
    d. ***Encouraging*** **people when they do things right** (such as providing recognition and praise when security is done well, and guidance when security is ignored or done ineffectively)
    e. ***Evaluating*** **how well people are doing** (for example, assessing whether the desired behaviours are being demonstrated as a matter of routine, and whether you are seeing increases or declines in important measures of success)

9. These activities can be achieved by using a range of interventions such as communication materials, behaviour change campaigns, training tools, existing organisational processes and other initiatives (e.g. induction programmes, management training), including managers and leaders role modelling the good practices. The messages can also be enhanced when they are ***Endorsed*** by credible experts.

10. Recent theory on delivering culture (and organisational) change encourages adoption of a top-down approach whereby a clear vision is set out and cascaded down through the layers of the organisation, ideally integrating into policies, systems, procedures and the fabric of organisation operations. For example, if organisational values and beliefs that security matters (such as that good security is essential to the success and performance of the overall organisation), are instilled then in turn this will shape employees to have a proactive attitude towards security (i.e. it matters and is something important) and will help to encourage the

demonstration of security savvy behaviours (such as locking computer screens, escorting visitors, and taking care over what is posted on social media about the working day). The benefits of this approach to improving security is that it aims to:

- Create shared values for everyone in the organisation around security
- Create relatively enduring and stable change
- Have a lasting impact on the way employees behave at work

11. Whilst the top-down approach continues to have much merit, in reality, this is a vast programme of work that is incredibly resource intensive and needs a level of coordination that is impractical for security teams (with limited resources, time and budget) to manage.

12. CPNI's Personnel and People Security Research and Development team have shifted to emphasise an alternative approach that is better suited and more feasible for CNI organisations and wider. This is a 'bottom-up' security behaviour change approach and involves a focus on identifying priority security behaviours, designing interventions to embed these behaviours, and monitoring and maintaining these over time. This builds a stronger security culture over a longer term wherein they will start to shape attitudes, and in turn start to change the *'way things are done around here*' and therefore the culture of the organisation.

13. Priority risks to your organisation's security and subsequently the key behaviours to reinforce or change can be identified through the use of a robust and frequently reviewed and updated risk register. Other methods of data gathering can be used also, such as interviews, surveys and focus groups with your staff.

14. This approach is more achievable and more practicable in organisations with a range of diverse groups or locations and among a workforce who move between organisations, meaning there is not always longevity in their security culture planning.

15. This approach requires a behaviour change campaign that is planned carefully and thoughtfully, in order that it works with the existing organisational culture and not against it. It is also important to consider how impact of behaviour change initiatives can be measured. Again, CPNI's 5E's 'evaluation' phase provides additional guidance on how this can be achieved, but ultimately, think about how this might be best achieved by you, within the particular context of the behaviour you are seeking to change.

16. Ideally, we can tackle the issue from both sides (top-down and bottom-up), and CPNI's 5E's to behaviour change provides the techniques to achieve this. In addition to the 5E's, CPNI has a range of off-the-shelf campaigns ready to use right now, alongside other supporting guidance such as the 'Pathway to developing your security culture – starting with behaviours', to be published by CPNI in Spring 2022.