The Importance of Security Culture in Facilitating Security Excellence: Does Culture Trump Strategy?

Security Research Initiative (SRI)

Professor Martin Gill
Charlotte Howell
Janice Goldstraw-White

July 2023

Perpetuity Research & Consultancy International (PRCI) Ltd
11a High Street · Tunbridge Wells · TN1 1UL · United Kingdom
www.perpetuityresearch.com
prci@perpetuityresearch.com
Tel: +44 (0)1892 538690

Copyright

Acknowledgements

We would like to thank everyone who has assisted us with our research. This work has been possible because of the ongoing support of our members and because the security sector has engaged with us. The members of the Security Research Initiative who sponsor the research deserve a very special mention. They not only sponsor, but their representatives also provide and share their experiences. They are: Mick Tabori and Joachim Ritter (Interr), Clint Reid (M&S), Barrie Millett and Jason Towse (Mitie), Steven Gardner (OCS), Richard Stanley (PwC), Imogen Hayat and Tony Holyland (SIA), Simon Pears and Jane Farrell (Sodexo). Clearly, they are not responsible for any of the views expressed in this report which are exclusively our own.

Our key supporters were once again invaluable in promoting the work. ADS (especially Jon Gray), ASIS (especially Rich Stevens), the BSIA (especially Mike Reddington and Andrew Cooper); IFPO UK & Ireland (especially Mike Hurst); IPSA (especially Simon Pears and Jane Farrell); the Security Institute (especially Angela Vernon-Lawson); and The SASIG (especially Martin Smith and Danny King); they are valuable advocates of the Security Research Initiative. So too our longstanding enthusiasts from security media: Roy Cooper and Mark Rowe (Professional Security Magazine), Brian Sims (Security Matters), Byron Logue (Infologue), and James Thorpe (Security Journal UK).

In establishing an understanding of the key issues we conducted a range of exploratory interviews and we are grateful for all those who took part. They by necessity must remain nameless but their role has been crucial and we are grateful.

We would also like to thank those who supported the research by promoting the survey among their networks: James Moore (IFSEC Global), Richard Jenkins and Dianne Gettinby (NSI), Chuck Andrews (Friends of Chuck). We would also like to thank all of those who took an interest in the topic and promoted the survey among their individual networks.

We owe a special thanks to all those (anonymous) contributors who gave their time completing our survey and who contributed insights and took part in interviews. They too, by necessity and agreement must remain nameless, but we acknowledge their important contribution here.

Finally, thanks to our colleague Claire Tankard for administrative assistance.

SRI Members

Executive Summary

The aim of the research was to explore the challenges to building a strong security culture in today's world and assess how the security sector is responding. It is based on the views of security professionals from in-house and contract positions, as well as other security experts, collected via an online survey and through one-to-one interviews.

Key findings from the survey

Factors that are important to delivering successful security operations

- The vast majority of respondents (96%) rated 'a strong security strategy' as important or very important to a successful security operation at an organisation.
- 'Effective security leadership' (83%), 'clear security objectives' (83%), 'an effective security strategy' (82%) and a 'strong security culture' (82%) were the factors most commonly rated as very important to a successful security operation.

The significance of security culture

- Three fifths (60%) of respondents indicated security 'culture' is as important as security 'strategy'; just under a third (32%) indicated security culture is more important than security strategy.
- Breaking this down by role, in-house security leads were the only group that most commonly viewed security culture to be more important than strategy.
- Views were mixed as to whether you can have a strong security culture without a strong broader organisational culture. Half (50%) disagreed; a little less (44%) indicated it is still possible to have a strong security culture without a strong organisational culture. Although respondents in a management type role were a little more inclined to believe the two were linked than those in an operative/officer type role.

Engaging the workforce with security

- Respondents most commonly believed the wider workforce of an organisation carry out behaviours indicative of a strong security culture at least sometimes (ranging between 31% and 42%).
- Two thirds (66%) indicated that 'employees value physical measures in their workplace' often or always.
- Less than half (46%) indicated that 'employees share a belief that security plays an important role in the organisation's overall success' often or always.
- Similarly, 43% indicated that 'employees view *contributing to a secure workplace* to be part of their job description' often or always.
- Just over a third (36%) indicated that '(where relevant) other teams/departments involve security in their projects early on' often or always.

Factors that support or impede a good security culture

- Over four fifths (81%) indicated that often or always 'security management personnel are positive ambassadors for security'
- Whereas fewer, close to three fifths (58%) thought the same was true of 'organisational leaders'.
- Just over half (52%) indicated that 'leaders are effective at communicating with the wider workforce in a way that engages them with the value of security often or always. Perhaps unsurprisingly then, just under half (46%) indicated that often or always 'the wider workforce of the organisation is willing to engage meaningfully with security requirements'.
- Close to two thirds (64%) indicated that often or always 'the overall values of the organisation support good security'.
- Contracted operatives indicated some of these factors were present less often than those in other role types did.

The impact of recent trends on creating a strong security culture

- 86% agreed or strongly agreed that 'when security teams are understaffed, it is more difficult to maintain a positive security culture'.
- 80% agreed or strongly agreed that 'cost cutting reduces the priority that can be attached to developing and maintaining security culture'.
- 77% agreed or strongly agreed that 'high levels of staff turnover and the use of temporary staff are making it harder to ensure everyone follows security requirements'.
- 63% agreed or strongly agreed that 'when the workforce of an organisation is dispersed (across lots of locations) it is harder to check whether people are engaged with security requirements'.
- 46% agreed or strongly agreed that 'the workforce of an organisation are generally more focused on requirements for cyber/information security than physical security'.

Barriers to achieving a positive security culture

- Respondents indicated a number of potential barriers including, lack of senior level 'buy-in', lack of financial investment, a negative perception of security, lack of or ineffective communication on security issues, complacency and apathy among the wider workforce of an organisation, turnover of staff and other staffing challenges, competing priorities and workloads among the wider workforce, the quality of security staff and of security management.

Key findings from the interviews

How significant is security culture?

- Interviewees typically felt that it was not possible to effectively implement a security strategy without a good security culture. They felt that culture brought life to strategy and defined the extent to which strategy is executed.
- There was some suggestion that security culture had become more important to a successful security operation than it was in the past, and

that to be successful the security culture had to provide a good 'fit' to the specific needs of the business and the context in which it was operating.

Is 'security' culture defined by 'organisational' culture?

- Interviewees typically believed there to be a relationship between security culture and organisational culture and that a good organisational culture enables a good security culture, while a bad organisational culture creates challenges for a good security culture.
- Some interviewees suggested that in some sectors the link between the two may be weaker, for example where the sector is heavily regulated or where the success of a company is less dependent on 'people'.
- Some thought it may be possible to overcome a 'bad' organisational culture if you had the right expertise and focus to drive a good security culture.
- Conversely, it was also flagged that a 'good' organisational culture is no guarantee of a good security culture.

Aligning security contractor culture

- Some interviewees suggested that security companies adapt to the client's culture in order to achieve alignment.
- Some noted that the commissioning process gave the opportunity to ensure the supplier and the client were a good fit which smooths the transition to aligning cultures.
- The need to integrate contracted officers into the culture of the client organisation was generally considered to be an important step and that this required treating contracted officers in a way that results in them feeling like a valued part of the client organisation.
- Alignment was generally seen to be more straightforward where staffing is stable. Interviewees saw security sector churn and ad hoc working at different client locations as making it much harder to achieve alignment on culture.
- Interviewees suggested that where a client organisation sees security as 'outsourced' and therefore 'separate' this was typically a barrier to alignment.

The main difficulties for creating a good security culture

- A key difficulty was organisations, leaders and the workforce not valuing security. The need for 'bad' things (a crisis) to happen to demonstrate the need for security, the negative perception of security as a barrier rather than an enabler, and the perceived under-investment in security were all viewed as factors that feed the perception that security is not important.
- Closely linked was gaining endorsement by the leadership of the organisation. Interviewees noted that if they do not take security requirements seriously, no one else will. There is a need to show not only how security will protect the organisation, but how security will support operations and enable the organisation to be successful, to be profitable.

- Communication was also considered to be a key difficulty. The main challenges here included: ensuring security messages are heard and prioritised; conveying why security requirements are important and what the benefit is to the workforce in order to engage people; demonstrating that compliance with requirements has been worthwhile and encouraging this to continue.

The impact of recent trends on security culture

- Trends that interviewees felt may benefit a security mindset, tended towards the type of issues that attract a lot of attention – 'crisis' type events, such as the recent pandemic, terrorism and protests. It was noted that as these threats have become more recognised by organisations, security's role in addressing them helps to demonstrate the value of security and thereby the need to engage.
- Trends that interviewees felt may undermine a security mindset included:
    - the increased use of 'working from home' which some felt has raised the risks to the security of employee devices, made the nature of securing people and property more complex, and resulted in some 'skills fade' where employees are less engaged in security practices because they spend less time in the office;
    - current financial pressures that may be leading organisations to spend less on security and therefore compromise quality; and further, financial pressures can increase the violence and abuse that the workforce are exposed to, which can compromise a positive security mindset and ultimately culture;
    - the number of recent social movements that some suggested may be reducing respect for authority, and by extension security and creating disruptions and distractions that work against a positive culture.

Overall, the findings suggest a strong security culture is at least as important in achieving excellence as a strong security strategy, indeed, both are required components of excellent security provision. Yet when it comes to creating a strong security culture there remains considerable scope for improvement in engaging people. Further, with recent trends come some familiar challenges (such as financial issues) but also some new ones (such as working from home) which serve to illustrate the point that there is no room for complacency – a strong security culture is not static – it requires ongoing commitment. It was clear that key to engaging people with a security mindset is articulating the value of security in ways that are meaningful to different audiences and not least senior leadership and security operatives as well as the wider workforce. Crucially, this means conveying the message that the security strategy and requirements that support it, are not just for a crisis, important though that is, but every day, as an enabler of operations and a contributor to the success of an organisation.

Table of Contents

Section 1. Introduction

1.1. In recent years there has been a strong focus on understanding what makes security effective; specifically to address the factors that distinguish the really good or outstanding from the merely average. It is clear these factors differ for different stakeholders. For example, for clients these include: understanding the key threats; having an effective security strategy; and having objectives aligned with the company. For suppliers these include: a strong focus on customer needs; skilled and motivated staff; and understanding the value-added proposition of the security service.[1] And all too often the primary factor contributing to success has been seen to be a strong and effective strategy that has the support of the Board and is implemented effectively throughout, but is it?

1.2. There is a famous quote attributed to management consultant Peter Drucker (citation unknown) that '*culture eats strategy for breakfast*'. In short that a unified and shared set of security values are the cornerstone of effective security, the glue that facilitates and enables outstanding performance. If so, there is evidence to suggest that there is a problem for security. One recent global assessment of security culture,[2] produced the striking finding that, of the industries explored, all were rated as having a 'Moderate' security culture, none were rated as 'Good' or 'Excellent'.[3] None!

1.3. Certainly, there are distinct features of security practice that may impede its ability to generate a benign security culture. They include:

- The increasing practice of organisations working from home, requiring different approaches as well as different practices in building a shared commitment to excellence
- Different organisational departments viewing security differently, having different needs for it, and viewing it variously as either an impediment to achieving (their) objectives and/or an unwelcome financial burden
- Differences between organisations and their security contractors – perhaps having different cultures (even competing ones) but anyway

[1] Gill, M. and Randall, A. (2014) *Aspiring to Excellence: The case of security suppliers and corporate security*. Security Research Initiative Study. Tunbridge Wells: Perpetuity Research.

[2] The elements measured include:
Attitudes: The feelings and beliefs that employees have toward the security protocols and issues
Behaviors: The actions and activities of employees that have direct or indirect impact on the security of the organization.
Cognition: Employees' understanding, knowledge and awareness of security issues and activities.
Communication: The quality of communication channels to discuss security-related topics, promote a sense of belonging and provide support for security issues and incident reporting.
Compliance: The knowledge of written security policies and the extent that employees follow them.
Norms: The knowledge of and adherence to unwritten rules of conduct in the organization.
Responsibilities: How employees perceive their role as a critical factor in sustaining or endangering the security of the organization.

[3] KnowBe4 (2022) *Security Culture Report 2022, Global Trends in Security Culture* - https://www.knowbe4.com/organizational-cyber-security-culture-research-report

requiring two different entities with different structures to be aligned and engaged
- The increasing array and sophistication of technologies available transforming (but sometimes complicating) what is possible
- A growing emphasis on convergence (e.g. especially between physical, technical and cyber security)
- Challenges in recruiting and retaining staff especially on the frontline
- Financial pressures brought about by an adverse economic climate
- A public perception that security is a 'tainted' industry

1.4. Given these challenges the purpose of this research is to better understand:

- The importance of security culture in facilitating excellence. Is it the essential glue? Does it trump strategy?
- What the core elements of a modern security culture are
- The extent to which a positive security culture is dependent on the characteristics of the broader organisational culture
- The factors that most support and impede the creation and maintenance of a good security culture
- Who the key stakeholders are and the key route to engaging them
- The factors that facilitate security conscious behaviours
- Any barriers to implementing an effective security culture

1.5. The report on which this research is based incorporates a global survey and one to one interviews.

Section 2. Thinking about security culture

Setting the scene

2.1 The question 'what factors make a company successful?', is a different one, and potentially generating different responses to 'what factors make a company attractive to work for?' They overlap of course but while any Google search might suggest the former will focus on strategy, objectives, having a unique product or distinct service approach, and being able to make a profit, the latter might focus on renumeration packages, conditions of service, management styles, workplace rules and such like, in essence the culture. But to take one example, can a strategy ever be successful, if it is not underpinned by a positive culture? Can it be effective without a unified approach among all stakeholders across an organisation? Isn't this true of security as much as it is true of organisational life generally?

2.2 In this section we start to address some of the key learnings from prior studies drawing on research that covers different settings but focussing on security specifically. It starts by defining 'security culture' and seeks to explain why it has been considered important, and then what the characteristics of a positive security culture are. We finalise this section by looking at some of the challenges to implementing one effectively.

What do we mean by 'Security Culture'?

2.3 Defining security culture is not straightforward.[4] Different interpretations[5] have variously viewed culture as centring on security awareness; on compliance with security requirements; and on all staff sharing responsibility for security. KnowBe4 (2022)[6], in its research on global trends in security identify culture as being the combination of thought processes, knowledge, habits and behaviours. Core though is the notion of shared values as the following illustrate:

> *'Security culture refers to the set of values, shared by everyone in an organisation, that determine how people are expected to think about and approach security.'* [7]

> *'Culture is defined as people's shared attitudes, perceptions and beliefs. A common metaphor is comparing culture to an iceberg. Like an iceberg, culture is hard to see*

[4] See for example: Carpenter, P. and Roer, K. (2022) *The Security Culture Playbook – An Executive Guide To Reducing Risk and Developing Your Human Defense Layer*
Malcolmson, J. (2009) 'What is Security Culture? Does it differ in content from general organisational culture?', *43rd Annual 2009 International Carnahan Conference on Security Technology*. IEEE, Zurich.
[5] KnowBe4 (2020) *The Rise of Security Culture*
[6] KnowBe4 (2022) *Security Culture Report 2022, Global Trends in Security Culture* - https://www.knowbe4.com/organizational-cyber-security-culture-research-report
[7] CPNI (March 2021) *Security Culture* - https://www.cpni.gov.uk/security-culture

as most of it is hidden. Like an iceberg, culture is also hard to move.'[8]

2.4 For the purposes of this research, by the term 'security culture' we are referring to the shared values that have been adopted across an organisation to guide the approach of all employees in respect of security.

Why establishing a 'good' security culture is important, and what 'good' looks like

2.5 Earlier we referred to the famous Peter Drucker quote that '*culture eats strategy for breakfast*'. Prior research points to a number of reasons why security culture is considered significant. First, that a positive security culture contributes to '*supporting and enabling business'*[9]*.* Second, that establishing a strong security culture is a critical element of ensuring employees are '*security conscious'* and therefore act to protect assets and information[10]. Third, a strong security culture is likely to '*increase compliance with protective security measures'*[11] which in turn is more likely to mean that security measures are effective[12]. Fourth, in binding people to the bona fide ethos of the organisation it is likely to reduce the '*risk of insider incidents*'[13]. Fifth - closely linked to the previous points - encouraging the right types of behaviours amongst all stakeholders not least staff acts as a '*huge force multiplier, at a relatively low cost'* in improving resilience to threats and reducing vulnerability[14]. Evidently then, security culture is important because it can enable or inhibit the overall effectiveness of security within an organisation.

2.6 The Centre for the Protection of National Infrastructure in the UK (2021)[15] observes that there is no single 'best' culture – that what is best will depend on the organisation, its priorities and the threats it faces. Nonetheless there are some features that appear to point towards both good and bad practice.

2.7 A number of authors[16] highlight the importance of a good security culture being one that is adaptable, flexible to changing demands and priorities,

[8] Sptizner L (2021) *Why a Strong Security Culture?* - https://www.sans.org/blog/why-strong-security-culture/
[9] NCSC (2017) *Growing positive security cultures* - https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures
[10] CPNI (March 2021) SeCuRE 4: Assessing Security Culture – https://www.cpni.gov.uk/secure-4-assessing-security-culture
[11] CPNI (March 2021) *Security Culture* - https://www.cpni.gov.uk/security-culture
[12] Vierendeels, G., Reniers, G., va Nunen, K., and Pennet, K. (2018) 'An integrative conceptual framework for safety culture: The Egg Aggregatd Model (TEAM) of safety culture.' *Safety Science* 103: 323-339
[13] CPNI (March 2021) *Security Culture* - https://www.cpni.gov.uk/security-culture
[14] CPNI (April 2021) *Optimising People in Security* - https://www.cpni.gov.uk/optimising-people-security
[15] CPNI (March 2021) SeCuRE 4: Assessing Security Culture – https://www.cpni.gov.uk/secure-4-assessing-security-culture
[16] See for example
CPNI (March 2021) SeCuRE 4: Assessing Security Culture – https://www.cpni.gov.uk/secure-4-assessing-security-culture

be that relating to changing objectives, working practices, business operations or the threat environment. Factors that have been considered to be indicative of a 'strong' security culture include[17]:

- An organisation (and therefore staff) that prioritise security
- Strong compliance with security policies endorsed by organisational hierarchies
- An awareness and understanding of security issues
- Consistency and timeliness in carrying out security requirements
- Recognising security is a shared responsibility across the organisation and incorporating all stakeholders
- Establishing formal groups of people that help influence security decisions
- Security being embedded into the values of the organisation.

2.8 Spitzner (2021)[18] suggests the most common indicators of a strong security culture include:

- People feel safe reporting incidents, even if they caused it
- People include security as part of their job description
- Employees correct and help their co-workers to be more secure
- A shared belief that security plays a strong role in an organization's success
- People feel comfortable asking questions of the security team
- There are frequent requests for training or briefings on security, and security is invited to become involved in projects early on

2.9 To some extent indicators of a weak security culture are the opposite of those presented above. What is key is the attitude of the security team and especially its leadership. Spitzner (2021)[19] notes that with '*an arrogant, punitive or fear-focused security team you will have a weak or perhaps even toxic security culture*.' Similarly, Needham (2018)[20] refers to the psychological effect (known as the Pygmalion effect) that people tend to behave in the way that others expect of them, thereby expecting the worst, results in the worst. Therefore, messaging is key too; generating engagement means having policies and procedures which

Kruger, H., and Kearney, W. (2006) 'A prototype for assessing information security awareness', *Computers & Security* 25(4): 289-296

Martins, A., and Eloff, J. (2002) 'Information security culture' *Security in the Information Socity, IFIP Advances in Information and Communication Technology,* 86, ed. Ghonaimy, M., El-Hadidi, M., and Aslan, H. Boston: Springer.

Schlienger and Teufel (2003)

[17] See for example:

NCSC (2017) *Growing positive security cultures* - https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures

Carpenter, P. and Roer, K. (2022) *The Security Culture Playbook – An Executive Guide To Reducing Risk and Developing Your Human Defense Layer*

[18] Sptizner L (2021) *Why a Strong Security Culture?* - https://www.sans.org/blog/why-strong-security-culture/

[19] Sptizner L (2021) *Why a Strong Security Culture?* - https://www.sans.org/blog/why-strong-security-culture/

[20] Needham D (2019) *Building a positive security culture* - https://www.bcs.org/articles-opinion-and-research/building-a-positive-security-culture/

are easy to follow and meaningful for those that are impacted. Spitzner (2021)[21] for example, notes that, '*if you have relatively easy to follow, common sense policies communicated by an engaging and supportive security team, you will have a strong security culture.'* Meanwhile, Solomon & Brown (2021)[22] highlight the importance of effective communication in influencing compliance with requirements; the essence of a security culture.

2.10 There is however a striking characteristic about these definitions which serve to underplay its importance. They all focus on seeing a good security culture in terms of ensuring better 'protection' against threats and/or compliance with rules. Important though these are, security has moved. Modern interpretations have stressed the link between security being more than this, specifically by enabling organisations to make a profit, by facilitating positive trading conditions even, and perhaps especially, in the most adverse environments. [23]

2.11 In many ways we have to be careful of not simplifying this discussion to just a few issues; it is much more complex than that. What constitutes an appropriate security culture varies with context. To elucidate the issues further it is instructive to briefly look at some of the impediments that are recognised as hurdles to building strong cultures.

Challenges to implementing a 'good' security culture

2.12 Many tools that have been developed to support organisations to measure and then improve their security culture[24] recognise that there are many impediments to doing so effectively and perhaps evidenced by the KnowBe4 security culture survey noted earlier. Briefly examining these challenges is instructive.

2.13 First, some authors[25] have cautioned that embedding a strong security culture should not be thought of as a 'one-off' project or take a short-term focus, rather it should be seen as an ongoing challenge, always supported by as the CPNI (2021)[26] note, a '*clear vision as well as a*

[21] Sptizner L (2021) *Why a Strong Security Culture?* - https://www.sans.org/blog/why-strong-security-culture/

[22] Solomon, G., and Brown, I. (2021) 'The influence of organisational culture and information security culture on employee compliance behaviour', *Journal of Enterprise Information Management*, Vol. 34 No.4, 2021 pp1203-1228.

[23] Gill, M.L. (2022) Thinking about the benefits of security and the barriers to recognising them. In Gill, M.L. (editor) the *Handbook of Security*, third edition. Basingstoke: Palgrave.

[24] See for example:
CPNI (March 2021) SeCuRE 4: Assessing Security Culture – https://www.cpni.gov.uk/secure-4-assessing-security-culture
See also a review of different tools undertaken by: Sas, M., Hardyns, W., van Nunen, K., Reniers, G., and Ponnet, K. (2021) 'Measuring the security culture in organizations: a systematic overview of existing tools', *Security Journal* 34: 340-357

[25] See for example: Security Mentor (undated) *Tips to Improve Your Organization's Security Culture* - https://blog.securitymentor.com/tips-to-improve-your-organizations-security-culture

[26] CPNI (October 2021) *Embedding Security Behaviour Change* - https://www.cpni.gov.uk/embedding-security-behaviour-change

coordinated strategy'. Second, it always needs to start, as a number of sources[27] highlight, with effective 'endorsement' by a credible source, and '*must always be seen to be endorsed consistently from the top of the organisation*'.[28] If the endorsers are not senior, if they lack commitment, if they change and are not followed by advocates then an effective security culture is in jeopardy.

2.14 Third, and recognising that cultures need to adapt, research has highlighted a number of factors that need to be considered before making changes[29]:

- *'The objectives of the change (i.e. the vision or strategy)*
- *The size and scale of the change (i.e. the gap between where the organisation is now and where it needs to be)*
- *The actions to implement the change (i.e. the interventions)*
- *The organisational readiness for the change (i.e. it has the necessary time, resources and buy-in)*
- *The types of communication to be adopted to instigate change to the target audiences and key stakeholders (i.e. the communications strategy)*
- *The process for reviewing and evaluating the impact of the change (i.e. the measures of success and key performance indicators)'*

2.15 Fourth, organisations and industries can differ markedly.[30] Therefore, as the NCSC (2017)[31] warns, instilling a security culture requires a '*look at the systemic factors underlying the things people do day-to-day*,' itself dependent on understanding working practices and existing cultures across the organisation.

2.16 Fifth, and crucially, and another point emerging from the NCSC (2017)[32] is that the security culture of an organisation is '*intertwined*' with organisational culture. They note a number of factors likely to have an impact:

- *'Physical buildings: open plan, or private offices? Brightly coloured, or shades of grey? Staid and serious or bunting, bunting everywhere?*
- *How we organise: rigid hierarchies and working processes, or fluid task-based teams?*

[27] See for example: Security Mentor (undated) *Tips to Improve Your Organization's Security Culture* - https://blog.securitymentor.com/tips-to-improve-your-organizations-security-culture
[28] Security Mentor (undated) *Tips to Improve Your Organization's Security Culture* - https://blog.securitymentor.com/tips-to-improve-your-organizations-security-culture
[29] They advocate the 5 E's[29] approach to effect behaviour change: '*Educate why*', '*Enable how*', '*shape the Environment*', '*Encourage the action*' and '*Evaluate the impact*'.
[30] KnowBe4 (2022) *Security Culture Report 2022, Global Trends in Security Culture* - https://www.knowbe4.com/organizational-cyber-security-culture-research-report
[31] NCSC (2017) *Growing positive security cultures* - https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures
[32] NCSC (2017) *Growing positive security cultures* - https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures

- *What tools we use: clunky and unbending, or intuitive and fitting our needs?*
- *How we talk to each other: can you go and perch on the boss's desk for a chat any time you like, or must you make an appointment with her PA three weeks in advance?*
- *How we learn: most of us learn far more from our immediate colleagues than we ever do from formal training programmes. Do people around us normally follow the security rules and processes, or routinely ignore them?*
- *What we do when things go wrong: rush around looking for someone to blame, or pitch in and fix things?'*

2.17 The significance of this, is that efforts to improve security culture by changing behaviour are unlikely to succeed if they do not match with people's impression of "*how we do things here*". This itself is subject to change as organisations seek to meaningfully embrace diversity, work towards sustainable practices that are good for the earth, and support social causes. In a different way there has been a greater focus on wellness. To what extent has security embraced these? And as noted, to what extend as the role of security as a profit generator, rather than just a protector, brought about a change in cultural requirements?

Summary

2.18 Implementing an effective security culture is invariably a challenge, dependent on a variety of factors, requiring the meaningful engagement of different stakeholders whose priorities and focus will often not be security focussed, and has to take account of a myriad of contextual factors which are themselves subject to change and not always predictable.

2.19 This section has sought to highlight what a security culture is, why it is important, its key characteristics, and outline just some of the barriers to implementing one effectively. Yet largely absent from prior work, most of it conducted pre Covid, is any sense of its importance in facilitating excellence, including supporting broader organisational goals on the one hand and the barriers to success given modern challenges. Certainly, the evidence suggests, from global research, that achieving excellence has been illusory. In the following sections we report on findings which seek to examine the reasons why and paint a path to better practice.

Section 3. Survey Findings

The sample

3.1. A survey of security professionals was conducted in order to gain a better understanding of the significance of security culture. The survey covered the following key themes:

- The role of security culture in delivering successful security operations
- The significance of security culture
- The level of engagement of the workforce with security
- Factors that support and impede a strong security culture
- The impact recent trends have had on security culture
- Barriers to achieving a positive security culture

3.2. The findings are based on 258 responses[33].

3.3. In the introduction to the survey it was noted that – *We define 'security culture' as the shared values that have been adopted across an organisation to guide the approach to security of all employees.*

3.4. The majority of questions were multiple choice, some of which posed statements which respondents were invited to indicate their level of agreement or disagreement with. A small number of questions invited open text responses. All of the topics covered are condensed and summarised below.

3.5. In addition to the frequency responses to questions, analysis was undertaken to assess whether views differed by specific characteristics/sub-groups of respondents. Only those issues that were statistically significant are included in the discussion, evidencing a relationship between the variables (i.e. not occurring by chance). Key points are integrated into the main findings, and include perspectives by:[34]

- Role
- Views on whether security culture is 'as important as', 'less important than', or 'more important than' security strategy

3.6. The majority of respondents had been working in the security sector long-term – 79% for more than 10 years. The sectors most commonly indicated by respondents as those they worked in (respondents could

[33] The number of responses to each question varies as some respondents dropped out part way through and some chose note to answer certain questions.
[34] While statistical tests were also undertaken against the remit of the respondent (e.g. local, regional, national, global etc) and the length of time the respondent had worked in security, responses were rarely affected by these characteristics.

tick all that apply) were Public Admin, Other Services and Government (33%, n=86), Retail (32%, n=82) and Property (31%, n=81). Over two thirds of respondents worked for organisations based in the UK (72%, n=171). Full breakdowns for length of time working in security, sector and country are provided in Appendix 2 (Table 2, 3 and 4 respectively).

3.7. Just over half of the respondents (53%, n=136) worked for a supplier; while a third (34%, n=87) indicated they worked for a buyer/customer.

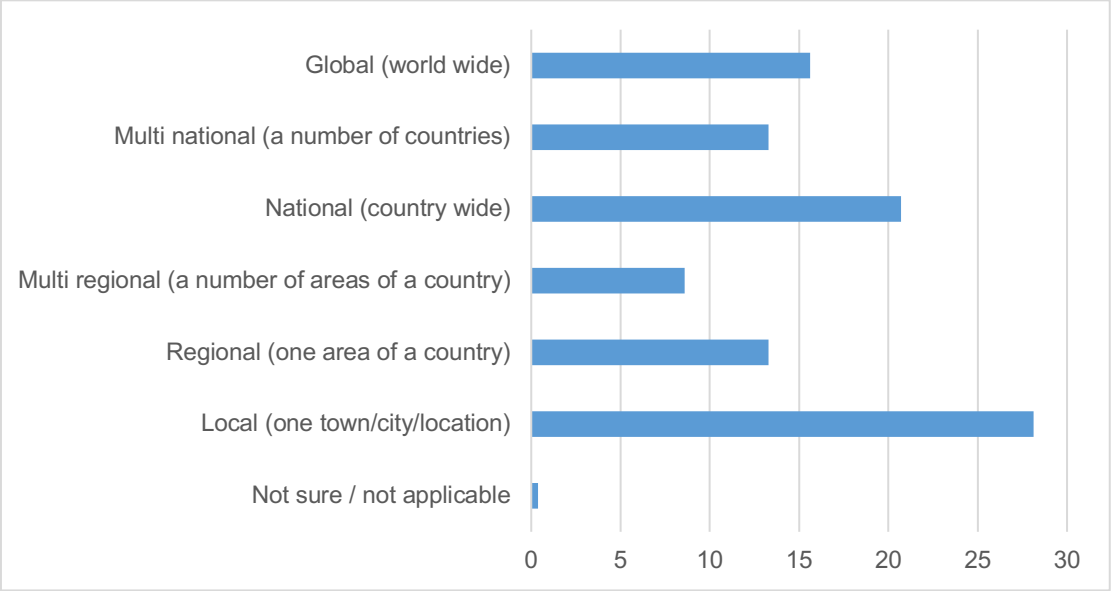
3.8. The remaining respondents were other security experts (e.g. academic, regulator, security association etc) at 9% (n=24) of respondents, or another interested party linked to security at 4% (n=11). Table 1 displays these roles.

Table 1: Breakdown of respondents by role % (n=258)

Role	Type	% , N	Total
Supplier	Director, Manager, Consultant	33%, n=86	53%, n=136
	Contracted operative	19%, n=50	
Buyer/ Customer	Security Lead/Manager	13%, n=33	34%, n=87
	Intermediary	2%, n=4	
	In-house operative	19%, n=50	
Other	Other security expert	9%, n=24	13%, n=35
	Other interested party	4%, n=11	

3.9. The remit of respondents varied considerably; more than a quarter (28%, n=72) had a local remit (i.e. one town/city/location), a fifth (21%, n=53) had a national remit (i.e. country wide) and 16% (n=40) had a global remit (i.e. world-wide). The full breakdown is shown in Figure 1.

Figure 1: Remit within current role % (n=256)



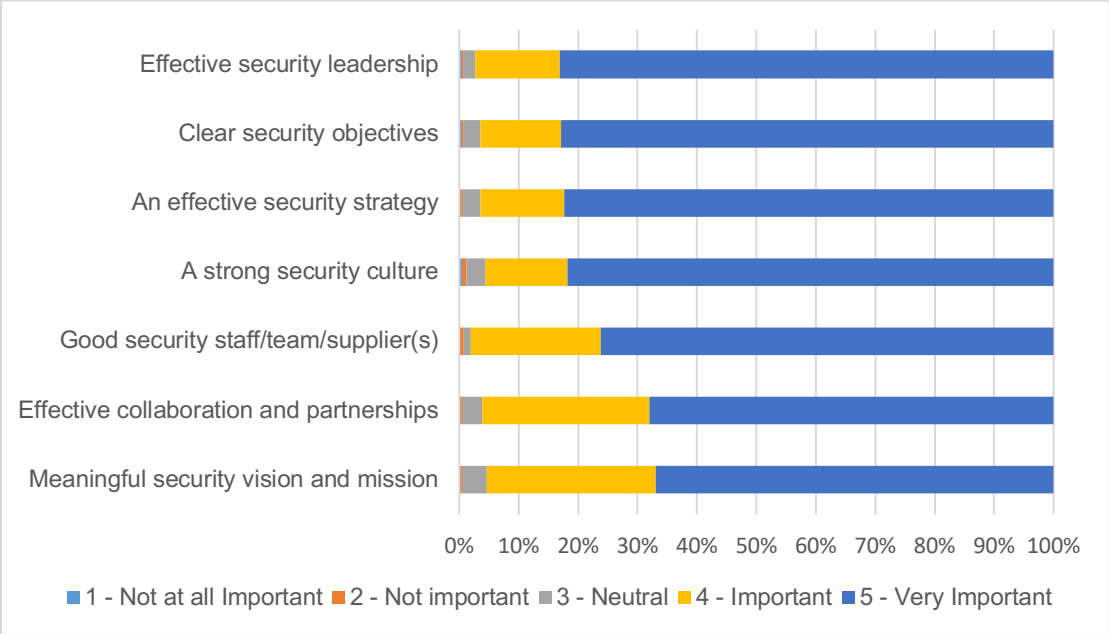
Factors that are important to delivering successful security operations

3.10. When asked about a number of factors that may be important to a successful security operation at an organisation, the vast majority of respondents (between 95% and 98%) rated each as 'important' or 'very important'.

3.11. Focusing on the factors that were considered **very** important, 'effective security leadership' (83%), 'clear security objectives' (83%), 'an effective security strategy' (82%) and 'a strong security culture' (82%) were the factors mostly commonly rated as very important.

3.12. Three quarters of respondents (76%) rated 'good security staff/team/suppliers' as very important, and around two thirds rated 'effective collaboration and partnerships' (68%) and 'meaningful security vision and mission' (67%) as very important. Figure 2 displays the results.

Figure 2: Importance of different factors to delivering successful security operations % (n=252-257)



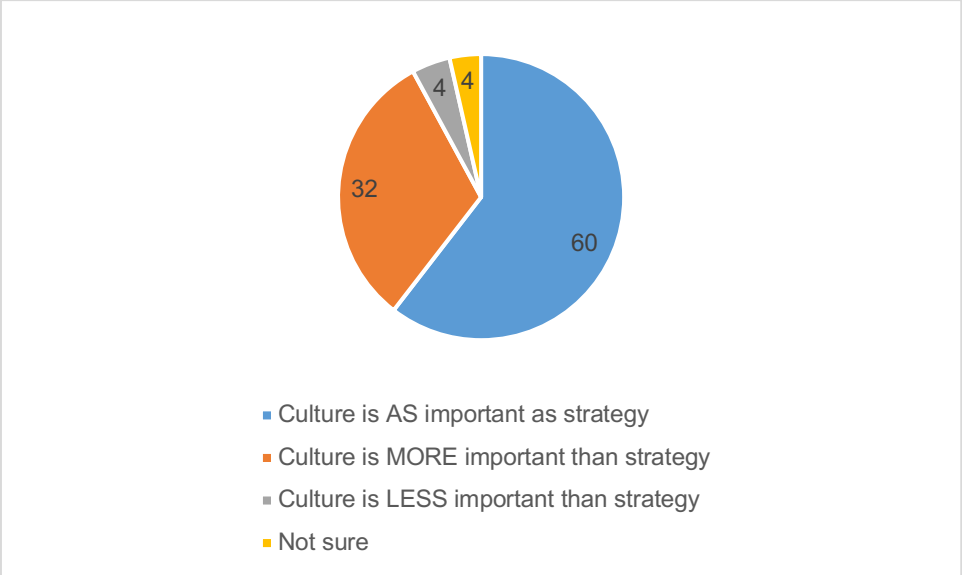
3.13. It was notable that contracted security operatives were less inclined to rate an 'effective security strategy' as important or very important (88%) than in-house security leads (buyers of security) (100%), management from security supplier companies (99%) and in-house operatives (96%).

3.14. Those that viewed security 'culture' to be l**ess** important than security 'strategy', valued factors such as 'good security staff/team/supplier' (91%) and 'effective collaboration and partnerships' (91%) much more than factors such as 'culture' (55%) and 'strategy' (73%).

The significance of security culture

3.15. To explore the concept of whether *culture eats strategy for breakfast* in the context of security, respondents were asked whether security culture is 'more', 'less' or 'as' important as the security strategy in the context of achieving a successful security operation. Three fifths (60%) of respondents indicated security culture is 'as' important as security strategy, and just under a third (32%) indicated security culture is 'more' important than security strategy. This is shown in Figure 3.

Figure 3: Whether security culture is more, less or as important as security strategy % (n=253)

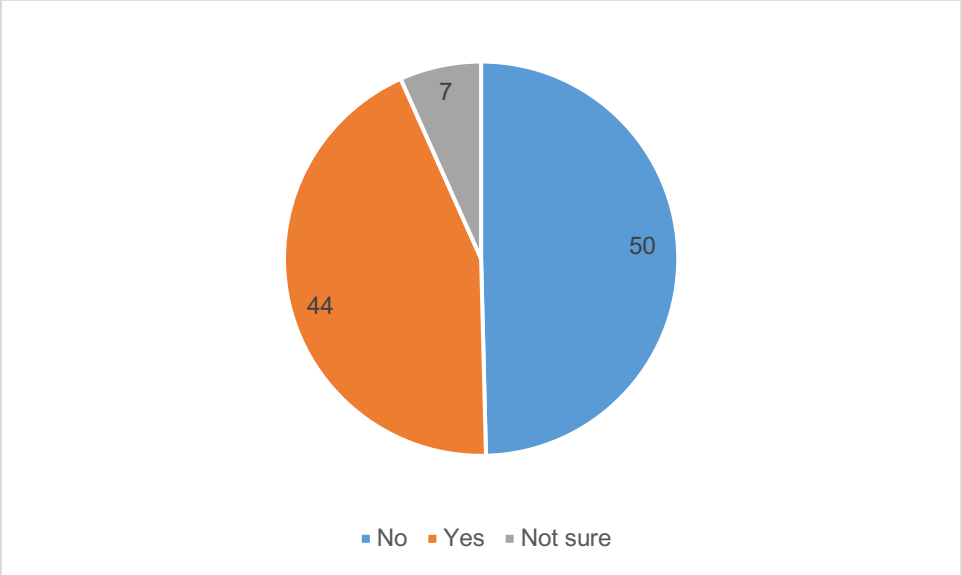


3.16. Notably, in-house security leads (buyers of security) were the only group that most commonly viewed security culture to be 'more' important than security strategy (57%). All other role types most commonly viewed security culture to be 'as' important as security strategy.[35]

3.17. Further, to explore the possible relationship between security culture and the broader organisational culture, respondents were asked whether you can have the former without the latter. Views here diverged; half of respondents (50%) indicated 'no' – that you need a strong organisational culture to have a strong security culture; a little less (44%) indicated 'yes' – that it is still possible to have a strong security culture without a strong organisational culture. This is shown in Figure 4.

[35] 67% of management from security supplier companies, 58% of contracted operatives and 56% of in-house operatives viewed culture to be 'as' important as strategy.

Figure 4: Whether it is possible to have a strong security culture without a strong organisational culture % (n=254)



3.18. While respondents in each different role were fairly evenly split in their views (for example among in-house operatives 50% answered 'yes' and 44% answered 'no'); it was notable that a small majority of 'managers' - both in-house security leads (buyers of security) (54%) and management of security supplier companies (61%) - answered 'no' (you need a strong organisational culture to have a strong security culture). Whereas a slight majority of those at the 'officer' level - contracted operatives (52%) and in-house operatives (50%) – answered 'yes' (it is still possible to have a strong security culture).

Engaging the workforce with security

3.19. The survey explored the experiences of security professionals in respect of the common indicators of a strong security culture. Respondents were asked to indicate how often behaviours of the wider workforce take place in the organisation they work for (or their general impression across the organisations they work with, where they work with a number of varying organisations).

3.20. For nearly all of the (7) behaviours explored the single most prevalent response was these happen 'sometimes' (ranging between 31% and 42%). For each behaviour, less than a quarter of respondents felt they 'always' happen, although most rare was the view that they 'never' happen (5% or less indicated they 'never' happen). If we assume that the ideal is that the behaviours 'always' happen, then based on these findings we can also assume generally speaking that security culture is not as 'strong' as would be desired.

3.21. Looking at the behaviours explored by the survey in further detail, it was notable that two thirds (66%) of respondents indicated that 'employees value physical measures in their workplace' **often** or **always**.

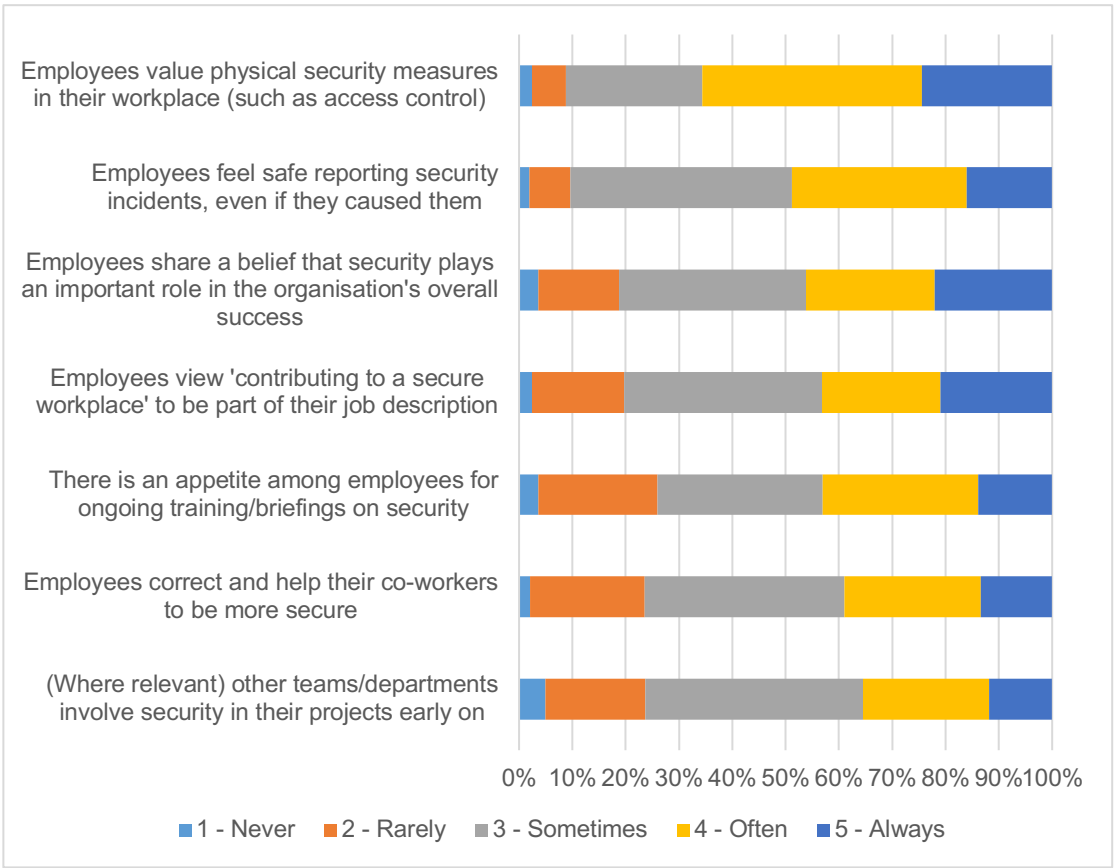
3.22. Just under half of respondents indicated that often or always 'employees feel safe reporting security incidents, even if they caused them' (49%), and that 'employees share a belief that security plays an important role in the organisation's overall success' (46%).

3.23. A little less – just over two fifths indicated that often or always employees view 'contributing to a secure workplace' to be part of their job description (43%), and that 'there is an appetite among employees for ongoing training/briefings on security' (43%).

3.24. Least common – less than two fifths indicated that often or always 'employees correct and help their co-workers to be more secure' (39%), and that '(where relevant) other teams/departments involve security in their projects early on' (36%).

3.25. The full breakdown is shown in Figure 5.

Figure 5: How often behaviours of the wider workforce take place % (n=245-250)



3.26. There were some notable findings here in respect of the answers of respondents that viewed security culture to be 'less important' than security strategy:

- They were more inclined to indicate that 'employees view 'contributing to a secure workplace' to be part of their job description' often or always (60%), than those that viewed security culture to be 'as important' (42%) or 'more important' (40%) than security strategy.

- They were less inclined to indicate that 'employees share a belief that security pays an important role in the organisation's overall success' often or always (30%), than those that viewed security culture to be 'as important' (48%) or 'more important' (43%) than security strategy.

Factors that support or impede the creation and maintenance of a good security culture

3.27. Respondents were asked how often a number of factors that may affect security culture were present in the organisation they work for (or their general impression across the organisations they work with, where they work with a number of varying organisations).

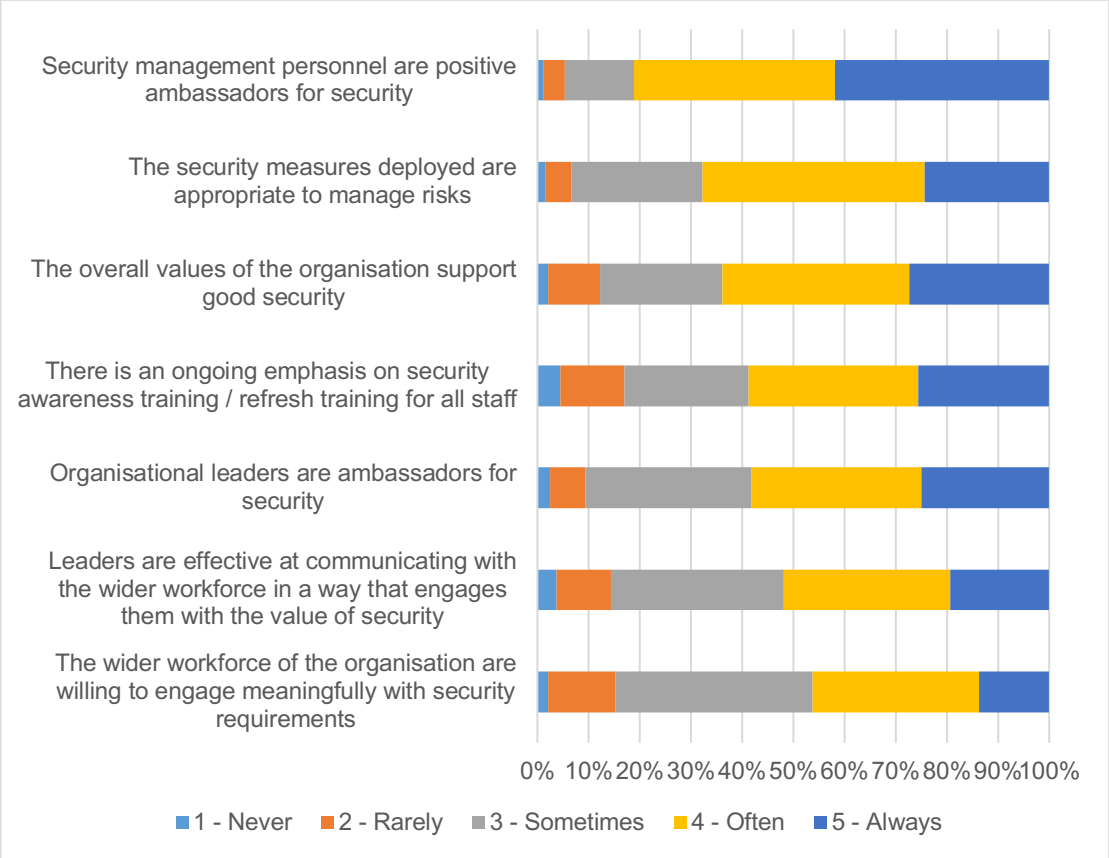
3.28. A large majority (81%) indicated that **often** or **always** 'security management personnel are positive ambassadors for security'. Less - close to three fifths (58%) - thought the same was true of organisational leaders (i.e. 'that organisational leaders are ambassadors for security'). And even less - just over half - indicated that often or always 'leaders are effective at communicating with the wider workforce in a way that engages them with the value of security' (52%).

3.29. Around two thirds of respondents indicated that often or always 'the security measures deployed are appropriate to manage risks' (68%), and that 'the overall values of the organisation support good security' (64%).

3.30. Just under three fifths indicated that often or always 'there is an ongoing emphasis on security awareness training / refresh training for all staff' (59%). Although, just under half (46%) of respondents indicated that often or always 'the wider workforce of the organisation is willing to engage meaningfully with security requirements'.

3.31. The full breakdown is shown in Figure 6.

Figure 6: How often factors that support or impede security culture are present % (n=238-244)



3.32. For some of these statements there was variation in responses by role, with contracted operatives indicating they are present less often than those in other role types:

- 'Security management personnel are positive ambassadors for security' – in-house security leads (buyers of security) were most positive (95% felt this was present often or always), both management of security supplier companies (85%) and in-house operatives (85%) were also very positive, but only 55% of contracted operatives felt this was present often or always.

- 'The security measures deployed are appropriate to manage risks' - in-house security leads (buyers of security) (83%) and in-house operatives (77%) were more positive (felt this was present often or always); compared with both management of security supplier companies (61%) and contracted operatives (57%).

- 'The overall values of the organisations support good security' – only 37% of contracted operatives felt this was present often or always; compared with 78% of in-house security leads (buyers of security), 72% of in-house operatives and 61% of management of security supplier companies.

3.33. Respondents that viewed security culture to be 'less important' than security strategy were less inclined to indicate that 'security management personnel are positive ambassadors for security' often or always (67%), than those that viewed security culture to be 'as important' (86%) or 'more important' (78%) than security strategy.

The impact of recent trends on creating a strong security culture

3.34. In order to understand how recent trends may be impacting on security culture, a number of statements were posed that respondents were asked to indicate their level of agreement with.

3.35. Agreement was strongest with the statements that reflect current challenges to security staffing and budgets suggesting that these issues will have wider repercussions for culture:

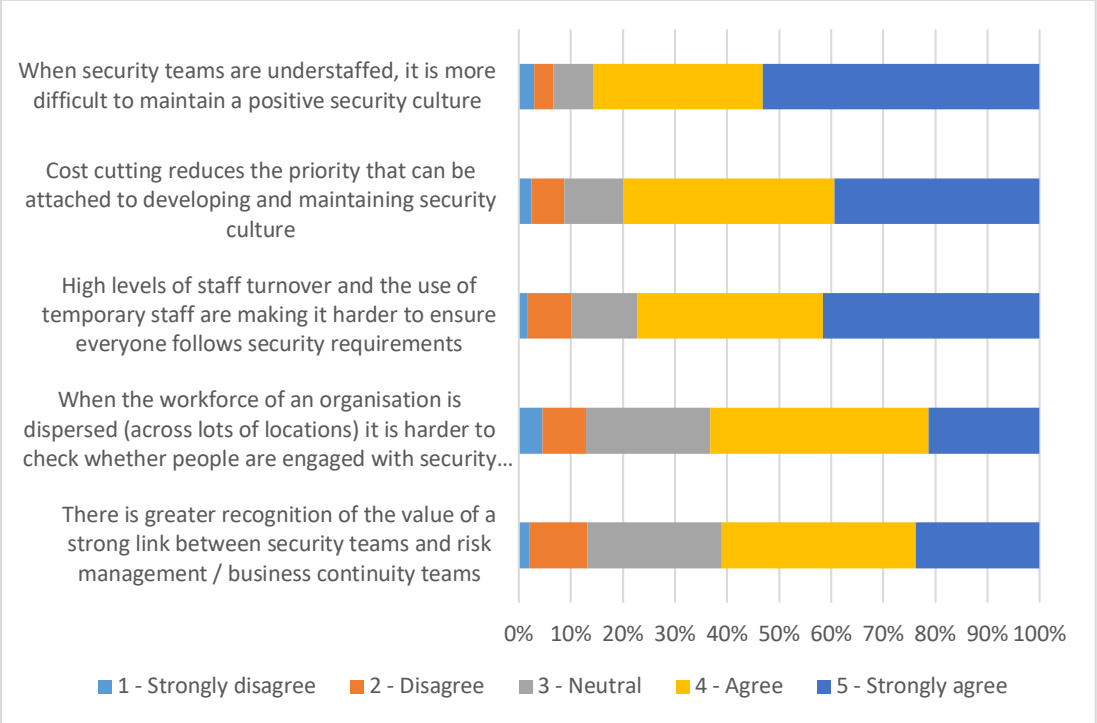
- 'When security teams are understaffed, it is more difficult to maintain a positive security culture' (86% 'agreed' or 'strongly agreed')
- 'Cost cutting reduces the priority that can be attached to developing and maintaining security culture' (80% 'agreed' or 'strongly agreed')
- 'High levels of staff turnover and the use of temporary staff are making it harder to ensure everyone follows security requirements' (77% 'agreed' or 'strongly agreed')

3.36. And just over three fifths of respondents agreed with the following:

- 'When the workforce of an organisation is dispersed (across lots of locations) it is harder to check whether people are engaged with security requirements' (63% 'agreed' or 'strongly agreed')
- 'There is greater recognition of the value of a strong link between security teams and risk management / business continuity teams' (61% 'agreed' or 'strongly agreed')

3.37. Figure 7 displays these findings.

Figure 7: The impact of recent trends on security culture – statements with the highest level of agreement % (n=236-239)



3.38. There were a number of the statements where agreement was less strong, albeit still representing around half of respondents.

3.39. Just over half agreed:

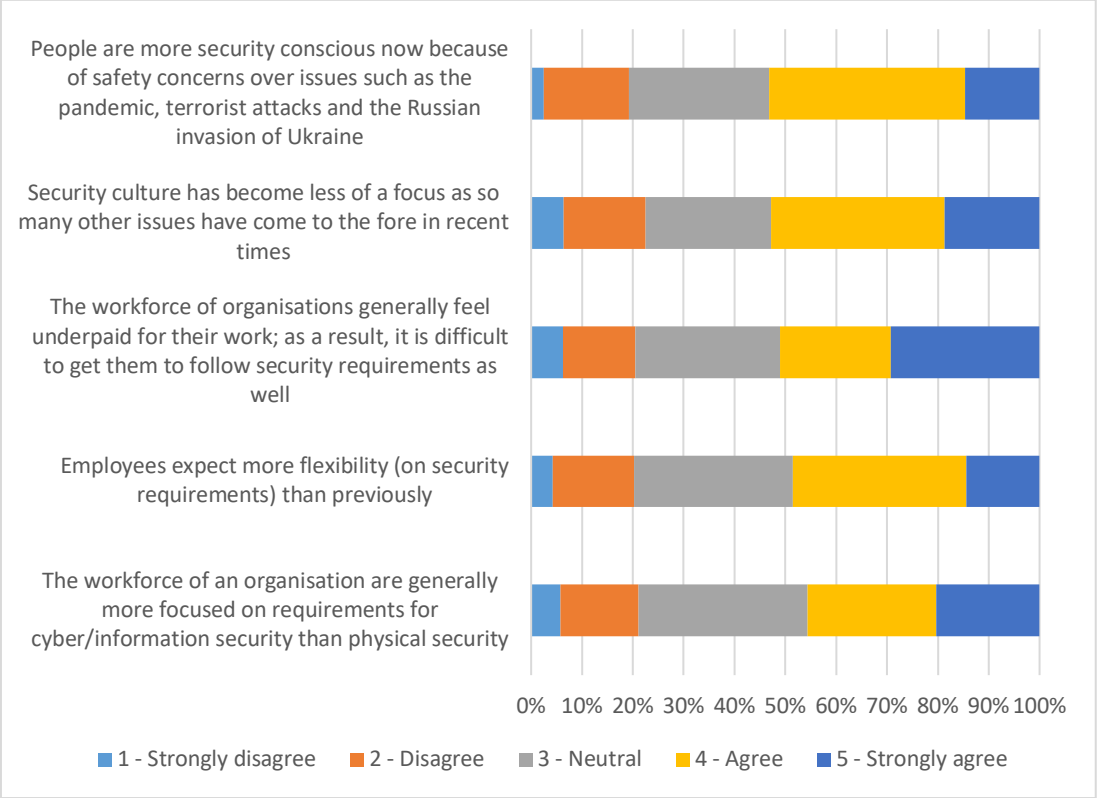
- 'People are more security conscious now because of safety concerns over issues such as the pandemic, terrorist attacks and the Russian invasion of Ukraine' (53% 'agreed' or 'strongly agreed')
- 'Security culture has become less of a focus as so many other issues have come to the fore in recent times' (53% 'agreed' or 'strongly agreed')
- 'The workforce of organisations generally feel underpaid for their work; as a result, it is difficult to get them to follow security requirements as well' (51% 'agreed' or 'strongly agreed')

3.40. And just under half agreed:

- 'Employees expect more flexibility (on security requirements) than previously' (49% 'agreed' or 'strongly agreed')
- 'The workforce of an organisation are generally more focused on requirements for cyber/information security than physical security' (46% 'agreed' or 'strongly agreed')

3.41. The breakdown for these statements is shown in Figure 8.

Figure 8: The impact of recent trends on security culture – statements with a lower level of agreement % (n=235-241)



3.42. Notably respondents with a global or multi-national remit were less inclined to agree[36] (than those with a national, regional or local remit) with the statement that 'the workforce of organisations generally feel underpaid for their work; as a result, it is difficult to get them to follow security requirements as well'. Meanwhile contracted security operatives were more inclined to agree (66%) with that statement and in-house security leads (buyers of security) were the least inclined to agree (28%).[37]

3.43. Further in-house security leads (buyers of security) were less inclined to agree than those in other role types that 'employees expect more flexibility (on security requirements) than previously' (31%)[38] and that 'security culture has become less of a focus as so many other issues have come to the fore in recent times' (44%).[39]

[36] 31% of those with a global remit and 34% of those with a multi-national remit agreed or strongly agreed; whereas 51% of those with a national remit, 67% of those with a multi-regional remit, 50% of those with a regional remit and 67% of those with a local remit agreed or strongly agreed.
[37] 66% of contracted security operatives agreed or strongly agreed; whereas 54% of management of security supplier companies, 48% of in-house security operatives and 28% of in-house security leads (buyers of security) agreed or strongly agreed.
[38] 31% of in-house security leads (buyers of security) agreed or strongly agreed; whereas 49% of management of security supplier companies, 51% of in-house security operatives and 56% of contracted security operatives agreed or strongly agreed.
[39] 44% of in-house security leads (buyers of security) agreed or strongly agreed; whereas 51% of in-house security operatives and 57% of both management of security supplier companies and contracted security operatives agreed or strongly agreed.

Barriers to achieving a positive security culture

3.44. Respondents were asked to indicate (in their own words) what factor(s) create the most significant barrier(s) to achieving a positive security culture. The themes are described below and are based on 195 responses although some respondents referred to more than one factor.

3.45. The most prevalent theme (n=63) related to the 'tone at the top' i.e. whether there was senior level 'buy-in':

> *'No buy-in from leadership (c-suite level).'*
>
> *(Survey respondent)*

> *'A lack of organisational leadership with a lack of understanding of the operational and commercial benefits that can be realised through a strong security culture and delivery.'*
>
> *(Survey respondent)*

> *'Engagement and commitment at Board/Exec level. Too many proposed strategies are either not fully or only partially supported which results in a lack of investment in people, equipment etc.'*
>
> *(Survey respondent)*

> *'If there are no security "champions" in leadership positions then it is an uphill struggle. Leadership has to be fully engaged and proactive if a security culture is to be encouraged, and to flourish and succeed.'*
>
> *(Survey respondent)*

> *'Weak governance, with no Board level accountable person for security.'*
>
> *(Survey respondent)*

3.46. For some this related to a general lack of understanding among senior leaders of the value of security:

> *'Lack of support from senior managers naively thinking security doesn't concern them.'*
>
> *(Survey respondent)*

> *'Lack of participative management where security is left to the security department.'*
>
> *(Survey respondent)*

> *'Many senior managers seem to want a security workforce that is seen, but not heard. Because many are focused on specific targets/goals, profit/loss of core business, they do not understand the value of an effective security function, until something goes wrong.'*
>
> *(Survey respondent)*

> *'Senior management not appreciating the value of security to the success of the company and just consider it to be another cost centre.'*
>
> *(Survey respondent)*

'Tendency amongst senior leaders to view security as the appendix of an organisation. They don't know what it is there for, but they know when it hurts. This drives a reactive culture and incident-based engagement with security.'
(Survey respondent)

3.47. For others it related more specifically to senior leaders not setting a good example in respect of specific security requirements:

'Seniors apply lip service only, setting a bad example.'
(Survey respondent)

'Not leading from the top down.'
(Survey respondent)

'VIP types bypassing security measures.'
(Survey respondent)

'The security culture not being driven by the senior leadership team, not demonstrating their adherence to the security culture, promoting it at every opportunity and not challenging those who fail to abide by the security culture.'
(Survey respondent)

3.48. Respondents commonly referred to a lack of financial investment (n=44) as a barrier. This mainly related either to a lack of investment generally in security and security officers, for example:

'Money. Security (in general) is the last to be invested in and the first to be cut.'
(Survey respondent)

'Security is typically underfunded therefore there is not the resources or talent to drive it.'
(Survey respondent)

'The appropriate resources being allocated to the delivery of security in support of the business objectives.'
(Survey respondent)

'Security costs money and there is a culture to pay low wages for a critical role.'
(Survey respondent)

'Low pay is a huge factor.'
(Survey respondent)

'Low pay rates attract officers that don't understand or want to understand the need for a positive security culture.'
(Survey respondent)

3.49. Or it related to lack of investment specifically in conducting activities to enhance security culture, for example:

'Funding allocation to build a sustainable and repeatable security culture.'
(Survey respondent)

'Lack of resource in some sectors means inconsistency and any messaging can be lost and or a positive culture does not have time to permeate and or embed.'

(Survey respondent)

3.50. A number of respondents (n=25) referred to the general attitude towards or perception of security across an organisation which meant there was no appetite to engage, for example:

'Negative view of a strong security culture.'

(Survey respondent)

'Sales motivated staff thinking it is a hinderance to achieving sales targets.'

(Survey respondent)

'Security is seen as a nuisance.'

(Survey respondent)

'The lack of interest in security as a general rule. Security can be seen as an obstacle to overcome rather than an entity to engage with and support.'

(Survey respondent)

'Them and us.'

(Survey respondent)

3.51. Meanwhile, a number of respondents (n=20) highlighted that issues with communication – such as a lack of communication or ineffective communication on security issues - can create a barrier to culture. Sometimes these were general communication issues but sometimes it was attributed to the way security teams communicate with others. Some illustrative examples include:

'Lack of communication. Not being able to reach unconnected workers.'

(Survey respondent)

'Lack of inter-departmental communication.'

(Survey respondent)

'Mainly communication. Staff can often undertake tasks or implement practices that affect security without consulting security. Similarly security can decide to implement security practices without consulting with either workforce or management.'

(Survey respondent)

'People responsible for security sometimes do not know how 'nice' they need to remain when instances of minor or major breaches take place within organizations. Frontline staff and their managers need to be trained how to communicate effectively to an employee, a visitor, a contractor or anyone else who might have come to the site/office and might not have followed security procedure of site/office.'

(Survey respondent)

'A significant barrier is the ability of the security practitioner to engage, explain, educate or influence the leadership and workforce to behave securely.'

(Survey respondent)

3.52. The same number (n=20) referred to issues of complacency and apathy among staff that meant there was a lack of focus on security requirements, for example:

'Apathy and familiarity, its easy to take your eye of the ball when busy with other matters.'

(Survey respondent)

'Individualism, egos, lack of care for others, self centredness.'

(Survey respondent)

'Not my job, others take care of that.'

(Survey respondent)

'Lack of shared responsibility- employees in general feel have no role to play in security.'

(Survey respondent)

People not taking ownership for security issues in their own places of work and ignoring minor security issues (lights broken, gate not locking etc.)

(Survey respondent)

'The perception of risk level is related to the experiences of the workforce within recent memory. Ironically, the more successful a security strategy is, the more complacent staff become about risks. This creates a constant challenge to reinvigorate the security culture.'

(Survey respondent)

'We've always done it that way.'

(Survey respondent)

3.53. The same number (n=20) also referred to the turnover of staff and other staffing challenges particularly with security staff:

'Constant turnover of security staff, meaning long term staff are constantly training new staff instead of concentrating on the job.'

(Survey respondent)

'Having a consistent and motivated team, driven by the challenges of reduced labour and, generally, uncompetitive pay rates.'

(Survey respondent)

'High staff turnover, generalised stigma between third party and in house staff and cut-backs in staffing levels due to better living wages and the price related to the economy.'

(Survey respondent)

'Under staffing, increased rate of turn-over, decreased morale, low job satisfaction.'

(Survey respondent)

3.54. Almost as many respondents (n=19) noted that staff have other priorities and high workloads which can affect their ability to focus on / comply with security requirements:

'Competing priorities for staff - meeting customer requirements and timescales against complying with security requirements.'

(Survey respondent)

'Getting the job done is still the priority; cutting corners on security is seen as a victimless crime.

(Survey respondent)

'Health and Safety, Fire Safety and Cyber (regulation) considered more important.'

(Survey respondent)

'Not giving people the time within their role to learn / be educated.'

(Survey respondent)

'Time, by this I mean people are perceived to be far too busy for basic security functions to be conducted.'

(Survey respondent)

3.55. A number of respondents (n=14) felt that the quality of security staff could pose a barrier, because officers that were poorly trained and/or demotivated would not be contributing towards a positive security culture, for example:

'I am seeing lots of Security Guards / Door Supervisor not having the basic level of communication skills in the English language (written or verbal).'

(Survey respondent)

'Having too many untrained, unmotivated officers on site.'

(Survey respondent)

'Private security industry per se is not so attractive for employment, hence number of people perceives it as a "temporary career until they find something better", and with that mindset there is greater challenge to get their buy-in and commitment at early stages of on-boarding and later refreshment trainings.'

(Survey respondent)

'Security don't value themselves or their role.'

(Survey respondent)

3.56. Some respondents (n=11) noted that security management was sometimes poor and where this was the case it posed a barrier:

'Lack of active engagement and leadership within in house security teams.'

(Survey respondent)

> *'Weak leadership. Lack of an overall risk mitigation and risk management strategy. Lack of effective middle management.'*
>
> *(Survey respondent)*

3.57. Other themes expressed by a relatively small number of respondents included a failure to ensure security measures are practical for the workforce of an organisation (n=7) and security departments lacking power and/or credibility (n=3).

Summary

3.58. Respondents were almost unanimous in their view that factors such as effective security leadership, clear security objectives, an effective strategy and a strong security culture are important in delivering a successful security operation. Indeed security culture, appears to be considered at least as important as strategy, and more so by some (and particularly in-house security leads). It was much less clear to what extent security culture may be at the mercy of the broader organisational culture (an issue we explore further in the next section) although those working at a more senior level (both in-house and suppliers) were a little more inclined to hold the view that you first need a strong organisational culture to be able to achieve a strong security culture, than those at the more junior level (both in-house and contracted operatives).

3.59. Feedback on how often behaviours and attitudes take place among the wider workforce that are indicative of a strong security culture indicated some positives. For example, two thirds reported a belief that employees value physical measures in their workplace 'often' or 'always' and across the behaviours explored a view that these 'never' take place was very rare. However, given how important security culture was perceived to be, the findings suggest there is considerable room for improvement in terms of engaging employees with security behaviours and attitudes. It was also striking that just under half of respondents reported that employees share a belief that security plays an important role in the organisation's overall success often or always. Of the statements offered to respondents, it was comparatively well supported. Yet it also shows how there is still more work to do, in making the link between what the security sector does and the contribution security makes to broader business objectives.

3.60. Looking beyond employee behaviours and beliefs to other factors that can support or impede security culture the picture was a bit more positive (although contracted operatives were at times less positive than those in other role types). A large majority of respondents thought security management are positive ambassadors for security often or always and close to two thirds felt the overall values of the organisation support good security often or always. Respondents were less confident that leaders are effective at communicating with the wider workforce to engage them

with the value of security and of the willingness of the wider workforce to engage meaningfully with security requirements.

3.61. There is some reason to believe that current trends may be impacting on security culture and therefore that this may be something to guard against. Current challenges relating to security staffing and budgets received the strongest levels of agreement in terms of having the potential to impact upon security culture. More generally, key barriers to achieving a positive security culture identified by respondents included: lack of senior level 'buy-in'; a lack of financial investment either in security generally or in enhancing culture; negative perceptions of security; weaknesses in communicating effectively in respect of security; complacency with respect to security requirements; staff turnover/staffing challenges; workloads/competing priorities among the workforce; the quality of security staff; and of security management.

Section 4. One to one interviews

Background

4.1. This section contains the findings based on 24 one to one interviews carried out with security professionals. Interviewees came from a number of countries and held a variety of positions including in-house and supplier/contractor views as well as consultants and other security experts. For context, an indication of role is provided against quotes included in this section but it should be noted that these have been anonymised.

4.2. The semi-structured interviews covered a number of topics relating to security culture: the significance of security culture and the implications of the wider organisational culture and the supplier culture; the main difficulties in creating a good security culture; and whether and how current trends may be impacting on security culture.

How significant is security 'culture'?

4.3. We asked interviewees how significant security culture is to a successful security operation and particularly whether the saying 'culture eats strategy for breakfast' applies to security.

4.4. The vast majority of interviewees felt that it was **not possible** to effectively implement a security strategy without a good security culture. They felt that **culture brought life to strategy** and defined the extent to which strategy is executed, for example:

> *'I think it's vital. It's probably not controversial to say you can have the greatest plans and strategy, world class procedures but if they are not followed the plans will stay on the shelf, it won't be effective.'*
>
> *(Interviewee 7, In-House Security Director)*

> *'Yes, I think it is true, you need the strategy but without the culture to embrace it, it can't work.'*
>
> *(Interviewee 20, Supplier – Senior Leadership)*

> *'I think the simplest way to express it is that people will resort to how they feel when acting and that is really about culture, and strategy is more black and white and does not deal with feelings.'*
>
> *(Interviewee 24, Supplier – Senior Leadership)*

> *'It is essential regardless of your organisation. It doesn't matter if you are a small business that has no interest in security. Or you are a global thing. A good security culture is the difference between you succeeding and failing. Any*

organisation needs a good security culture, otherwise it is exposed to increasingly a wide range of risks.'

(Interviewee 4, Other Security Expert)

4.5. One respondent disagreed in the sense that they felt it could still be possible to have good security with a bad culture, but their view was that a good security culture makes the process **easier**:

'Culture does not beat strategy, a good culture without strategy will not achieve anything, or at least very much. I stay away from black and white positions but if you are going to make people safe, then you need them on your side. You can't meaningfully do security to people it has to be done with them. So maybe you can do good security with a bad security culture, maybe, but it is much more difficult.'

(Interviewee 16, Security Consultant)

4.6. Another interviewee reflected on how the significance of culture had shifted, becoming **more important** to a successful security operation than it was in the past:

'I think culture has become more important as security has become more business minded. Once upon a time strategy was the be all and end all – when it was about gates, guards and guns – you needed a good strategy – you were putting the shell around the egg and what happened inside the shell was irrelevant. You were enforcing around an organisation. Now I would say it is completely the reverse. You can have the best strategy but if key stakeholders and employees are not bought in to it, then a really great strategy just becomes a piece of paper. Culture is more important now than it was – security has become more of a team sport.'

(Interviewee 11, In-house Security Director)

4.7. In a similar vein some interviewees talked about the need for security to be seen as a **business enabler** in order to set a culture that leads to a successful security operation:

'Culture is critical to success. You can put access control everywhere, but the importance of security access control is that when someone tries to access by say following the person in front closely you need the people to challenge them. That comes from a culture that has been set, and that is driven for me by not seeing security as a barrier to operations but as a business enabler.'

(Interviewee 14, Supplier – Senior Leadership)

'If you develop and implement a security plan in isolation from the rest of the business and it doesn't link into security culture, the plan fails at first contact. Because to have an effective security culture or regime in place in any

organisation, you can only do that if you have the buy-in of the business and security is an enabler to business.'

(Interviewee 8, Supplier – Senior Leadership)

4.8. Further, some interviewees talked about the **balance** that was required; that for security culture to support a successful security operation, it has to 'fit' with the needs of the business and be appropriate to the risks:

'It is a balance. What does the business need? We are trying to make sure the posture is commensurate with the needs of the business. If it is too aggressive people resent it. Security becomes seen as the people who said no. If you do that, eventually people don't ask you and then you don't know what they are up to. You only find out when it goes wrong.'

(Interviewee 7, In-House Security Director)

'I could make a 100% safe London underground system and remove the ability of someone to carry out a suicide bombing, but I would have to put in security measures such as you have at Heathrow or Gatwick. Would you want to report an hour before your tube train to go through security? You have security on one side and freedom on the other. Your job [as a security lead] is to explain where that seesaw is to the people on the c-suite that will be accountable for those decisions.'

(Interviewee 9, In-House Security Director)

4.9. On this point, one interviewee explained how within a single organisation, what the security culture looks like, may need to **vary in different settings** and contexts to achieve the right balance:

'We have different operations around the world. We overall are relatively permissive in terms of security. Most office locations, there is not that much exciting happening there. In other locations it is a more challenging environment, offices may be hit by earthquakes, typhoons, there are things going on to keep people's minds sharp. The culture around security and preparedness is far more mature there.'

(Interviewee 7, In-House Security Director)

4.10. The interviewee also talked about the value of being **able to scale security up and down** when appropriate and how this extends to culture in terms of the behaviours and awareness of the wider workforce:

'When the threat ramps up, to be able to ramp the posture up is quite powerful. You can't operate at 'critical' continuously. People burn out or start to cut corners. So that is quite a powerful thing to be able to do.'

(Interviewee 7, In-House Security Director)

4.11. A number of interviewees highlighted that an organisation is more secure when a **greater proportion** of the workforce is playing a part in security,

and that this only happens when there is a positive culture where the workforce understands and values security:

> *'It's the layers of an onion. The more layers you have, the more protected the centre is. If you have fewer layers or no layers, your centre is very exposed. People feel safer if they can contribute. You need people on the front line to be the eyes and ears. You need a culture where people feel empowered and understand the benefits of creating a more secure organisation.'*
>
> *(Interviewee 4, Other Security Expert)*

> *'Culture is critically important in helping people understand why we are all there.'*
>
> *(Interviewee 6, Supplier – Senior Leadership)*

> *'Generating a really good security culture is very effective because our business has 25,000 people. If they are on board with security, rather than just a small security team, life is made easier. If staff feel empowered and happy to challenge someone not wearing their pass in a polite and friendly way, then we are in a great place, rather than expecting the security team to be everywhere.'*
>
> *(Interviewee 7, In-House Security Director)*

> *'A risk-based approach is like a peach. The flesh has to allow employees, contractors, suppliers, threats, business continuity disruptions; it has to allow a certain amount through the flesh. But you have the stone in the centre where the crown jewels are locked up and completely secure. Culture defines what happens in the flesh of the fruit. You can't manage all those threats on your own. You need your people.'*
>
> *(Interviewee 11, In-house Security Director)*

4.12. One interviewee specifically warned that the success of a security operation can impact on the **organisation's overall success** and hence the role of culture is key:

> *'Ultimately without a good security culture an organisation will be less safe and less secure which can result in the right processes and procedures not implemented. It will impact on the safety of the organisations people, their customers, and also their assets – fixed assets or information assets. Which could ultimately impact the organisation's success.'*
>
> *(Interviewee 8, Supplier – Senior Leadership)*

Is 'security' culture defined by 'organisational' culture?

4.13. We asked interviewees to what extent the security culture at an organisation may be defined by the overall organisational culture.

4.14. Interviewees typically believed there to be a **relationship** between the two, and that a good organisational culture **enables** a good security culture because the mindset will be more conducive to good security. For example:

> *'They go hand in hand. One enables the other. A strong culture across the business will enable you to deliver a security culture. Trying to get the security culture without the organisation culture would be an uphill struggle.'*
>
> *(Interviewee 1, In-House Security Director)*

> *'I think you are because it is a mindset, there are certain cornerstones as to what makes an organisation tick.'*
>
> *(Interviewee 20, Supplier – Senior Leadership)*

4.15. And unsurprisingly, conversely, that a bad organisational culture creates **challenges** for a good security culture. For example:

> *'I don't think you can have a security culture without a good organisational culture. If that culture is top down, toxic etc then it is much harder to have a proper security culture.'*
>
> *(Interviewee 18, Other Security Expert)*

> *'Having an overall negative culture, breeds apathy, so while somebody – everybody has a desire to do a good job - but if they believe they are banging their head against a brick wall, they just go through the motions.'*
>
> *(Interviewee 10, Other Security Expert)*

> *'If there is an overall attitude where you don't mind a bit of corruption or law breaking, security is just an expense and you don't see the value – that permeates through every level of your organisation – it's dangerous.'*
>
> *(Interviewee 4, Other Security Expert)*

> *'Even if you have a good security culture but the general organisational culture wasn't good – you would lead with it and hope, but generally it would probably be pulled down as well eventually.'*
>
> *(Interviewee 12, Supplier – Senior Leadership)*

4.16. In a slightly different way, one interviewee gave an example where the organisational culture was not 'bad' per se, but was so fundamentally **conflicting** with attitudes that are typically conducive to good security that they thought this would pose a challenge:

> *'In the Tech sector – I've seen mantras inside places, like 'drive it like you stole it' and 'move fast and break things'. Where the culture of the organisation is directly opposed to the idea of controls.'*
>
> *(Interviewee 6, Supplier – Senior Leadership)*

4.17. One interviewee considered organisational and security culture to be interlinked at a more fundamental level; that the security culture is **a part of** organisational culture:

'To me [security] is just another strand of an organisation, security culture is part of the organisational culture as any other function is. I see security as a mainstream function, so if one aspect of the whole organisation is not good, then all the functions are not good, so I see them as entwined.'

(Interviewee 16, Security Consultant)

4.18. Another interviewee made a different point; that rather than the organisational culture hampering the security culture; that the security culture desired by security leads in the past had not always been **related well** to the organisation culture and that had its own problems:

'I think if you look back security culture and teams were run by ex-police and ex-military who bought security values of a certain type, now the focus is wider than that, that helps in terms of relating to an organisation, this is happening more and more and it has had to change. That is a good sign I think.'

(Interviewee 23, Other Security Expert)

4.19. A couple of interviewees suggested that while there was a link, there may be some **sectors where the link is weaker** and therefore you can have one without the other:

'My initial response is I don't think you can have a strong security culture if you don't have a strong business culture – maybe that is true when you are in a people business. There may be some – perhaps manufacturing or something heavily regulated, maybe there you can have a strong security culture without a strong business culture. I think where it is people, you can only have a strong security culture if you have a strong business culture.'

(Interviewee 11, In-House Security Director)

'Very interesting question that, and my immediate response is that it will depend on the sector. Security can sit outside the strategic delivery of a business but then it is not as effective as it should be.'

(Interviewee 14, Supplier – Senior Leadership)

4.20. Another couple of interviewees suggested that a 'bad' organisational culture could be **overcome** to generate a good security culture if you had the right expertise and focus:

'There are lots of other organisations where the strategy and cultural focus is increasing share price – it's all monetary focus. To shift the tide of that focus and make sure they blend safety and security in that culture – you need a strong personality at the helm and someone with a lot of experience and knowledge. They will be challenged, if you don't have the experience, you won't be able to change that focus until maybe an incident happens.'

(Interviewee 8, Supplier – Senior Leadership)

'If the client does not have a good culture, it is difficult. We took over a client and we knew we had to do something. We really focussed on turning them around and so you can work at a bad situation as we did here. It takes a real focus though but can be done.'

(Interviewee 21, Supplier – Senior Leadership)

4.21. In another way, a couple of interviewees flagged that the presence of other good cultures within an organisation was **no guarantee** of a good physical security culture:

'Almost every company has a strong IT security culture … Physical security is not so convenient. It is easier to make a challenge to a [phishing] email than to someone [in person] that you don't recognise ... when you confront people personally rather than anonymously online.'

(Interviewee 24, Supplier – Senior Leadership)

'I think security is wholly driven by the leadership, up and down. Without a good company culture, you can't create a security culture. The difference is that leadership promotes the values of the organisation but are less overt advocates of the security culture; often because they are ill advised or just don't understand [security].'

(Interviewee 15, Security Consultant)

Aligning security contractor culture

4.22. We explored with interviewees whether there are any specific implications to take account of for organisations employing contracted security, given that this has the potential to introduce a further culture (that of the security supplier company) into the mix.

4.23. A number of interviewees noted that (good) security companies typically **adapt** to the client's culture:

'With suppliers the culture varies greatly and depends on individuals. Some people's idea of security is a million miles away. If your name's not on the list, you're not coming in. That is not what we want – we want a softer, front of house approach for our culture. More open and friendly. That's the difference. Even in one specific guarding company you have individuals with all different mindsets. They don't try and sell a culture – they flex it to the client's culture.'

(Interviewee 1, In-house Security Director)

'If you look at the view of the guarding side of the house – that has to fit in to the culture of the customer.'

(Interviewee 6, Supplier – Senior Leadership)

'Outsourced needs to understand the client's culture and what you need to do is be able to articulate that to the security team.'

(Interviewee 10, Other Security Expert)

'Well if you are selling a professional skill you need to make sure you match it to the buyer's requirements.'

(Interviewee 22, Other Security Expert)

4.24. But one interviewee talked about the importance of not always going along with the client culture, and highlighted the **value of discussion** and debate:

'There can be a locking of horns, from a mature provider standpoint. A mature provider should have the confidence to challenge what is being pushed out from the in-house team. You should be able to debate what is appropriate. Lots of providers do slot in with whatever the client wants, to ensure they retain the contract. You need a mature supplier to be able to have those difficult conversations and debate the right approach. That is the best-in-class approach. I've worked with a number of clients with strong and experienced corporate security teams, that want to have informed debates. That is win win.'

(Interviewee 8, Supplier – Senior Leadership)

4.25. A number of interviewees flagged the need for the client organisation to take steps to i**ntegrate** contracted officers into their culture and it was apparent that a key part of this was to ensure that contracted officers are treated in a way that results in them feeling like a **valued** part of the client organisation. For example:

'I think for us, its successful where there is quite a few roles in our security teams that are wholly dedicated to [our organisation]. They feel like they have an identity as working for [us]. We treat our contractors the same as full time employees. It is a theme across the business. Partnership and team cohesion – you are part of our team, you get the same level of support and engagement from us, bring them in to the fold. I want people to feel invested to generate a better culture.'

(Interviewee 7, In-house Security Director)

If you are providing a positive environment, it is easy to motivate and inspire the contractors coming into that environment.'

(Interviewee 11, In-house Security Director)

'The facilities team had a one team approach – coming back to culture – building that positive culture as a business helps, because it is not an 'us and them' at that point.'

(Interviewee 11, In-house Security Director)

'It comes down to are they there to provide a service or are they invested as well. [A former company I worked for] had a long-standing relationship with their security partner and the two businesses were invested in each other. It may be much more of a challenge if you have a transactional relationship with your vendor.'

(Interviewee 11, In-house Security Director)

'At a famous company I know, in fact I had a meeting there, they have a big supplier and all the staff and all the security supplier staff were dressed the same, casually, the security staff looked like the client, I mean wearing the same relaxed clothes as they do, and that suggested to me an aligned plan and aligned operations and a good security culture.'

(Interviewee 18, Other Security Expert)

4.26. However, some interviewees sounded some caution around contracted staff becoming too embedded in the client organisation (although security managers more so than officers); while it is desirable for contracted staff to integrate to the client culture, losing all sense of the contractor culture can mean that the contractor loses good staff should the client and contractor go their separate ways. For example:

'The challenge for us is as a contractor, we are trying to impart our culture and our staff are on our clients' property and they want too want to impart their culture. It can be good, but if they do align with a client, we don't want them to forget our values. It can create problems. So we have to be careful we may lose our contract and it can be difficult to pull our best staff if they have a lot of loyalty to that property. Then it can be difficult.'

(Interviewee 24, Supplier – Senior Leadership)

'Where the contract security manager takes on the culture of the contract they are assigned to, in preference of the security company for which you work. That is largely true. [When I was in contract security] I took on the standards and culture that came from [a particular organisation] because I thought that was a better way.'

(Interviewee 9, In-house Security Director)

4.27. The feedback from interviewees suggested that the issue of alignment between the client culture and the contractor culture is **more straightforward** where staffing is settled, than where it is not:

'We contract security officers. They all adopt our culture. We have officers that have been here for 20 or 30 years. They have been TUPED across each time, that are embedded in our own culture.'

(Interviewee 1, In-house Security Director)

'100% when you have got ad hoc staff working once, twice a week, or working at different locations it is hard to create a culture.'

(Interviewee 2, Contracted Operative)

'The problem comes if you have industry churn; different guards, week in week out. They never come up to speed.'

(Interviewee 11, In-house Security Director)

'It does impact on the culture, take the security officer, who has an allegiance to the paymaster, and especially so where they are not working for one client as is the case with some contract workers.'

(Interviewee 15, Security Consultant)

4.28. A number of interviewees noted the relevance of selecting a supplier with an appropriate 'fit' as part of the **commissioning** process, so that the transition to align cultures is as smooth as possible:

'Cultural alignment. You need a company that has a similar fit to your own.'

(Interviewee 9, In-house Security Director)

'If you have a strong security culture and a strong business culture the types of vendor you will lean towards is probably quite similar to you, it will be important that there is a cultural fit to your organisation. There will be some differences but if you are partnering with the right vendor, it minimises that.'

(Interviewee 11, In-house Security Director)

'Actually in contracting in you can feed into your requirements. So if sustainability is key you make sure that you put that in your tender requirements.'

(Interviewee 23, Other Security Expert)

'It can be a challenge but that's part of the reason I get paid. It is my responsibility to ensure that is as seamless as possible. The client is there to ensure their values and mission statement are clearly defined so we can see the synergies. Generally they are samey. There has not been a case where they have wildly different world views.'

(Interviewee 3, Supplier – Account Manager)

4.29. And related to this it was noted that suppliers could take the initiative not to work with client organisations that do not have the right attitude to security to avoid engaging with a poor fit and poor culture:

'Some clients you would be better off not having. It is a brave organisation to choose not to trade with some customers.'

(Interviewee 10, Other Security Expert)

4.30. One interviewee flagged that the issue of alignment is less about using 'contracted' staff and more about individuals coming from different settings and contexts and needing to fit in to a different culture than what they were previously used to. Another made a similar point about

matching an individual's experience with the setting. Both examples follow:

> *'A lot of people doing security will come from a door supervisor background but security in say a football stadium is very different to in a nightclub. You spend the first few matches adjusting their culture to match and move away from the night-time economy. The same with health. The fact someone has a door supervisor licence and is good with dealing with conflict in a club, doesn't mean they are an ideal person to deal with aggression on a dementia ward. But if I took an in-house team from a nightclub, they would have the same problems. The culture and training they have had. The problem isn't that they are a contractor. It's the training they have already had doesn't cope with the nuances for other settings.'*
>
> *(Interviewee 9, In-house Security Director)*

> *'It is a matter of education. If we take a construction site security officer and place that person in corporate head office there is a mismatch, so you need to manage who and how security is provided, it is not just a bum on a seat it has to be appropriate for that environment. The management of security officers is a challenge because of the pay and the type of person but all the more reason to match.'*
>
> *(Interviewee 14, Supplier – Senior Leadership)*

4.31. In a similar vein to the point about integrating contracted officers, a number of interviewees observed the difficulty in aligning cultures where the client organisation sees security as 'outsourced' and 'separate' and **does not feel a need** to integrate the security contractor into their organisation:

> *'We are contractors and we have a culture and ideally we should all be the same. Ideally that is. Most often we are not aligned. A security company can still fulfil its function and have a good security culture. The problem is that we lack proactivity from the client and it is oil and water and they don't mix. It is luck of the draw with clients, some clients want proactive security and some don't, some, they just see security as a body.'*
>
> *(Interviewee 19, Supplier – Security Manager)*

> *'The problem we have is people take the attitude that I've outsourced this so it's no longer my problem. That is a dangerous mindset. That security officer should be part of your team. You end up in a scenario where no one cares.'*
>
> *(Interviewee 4, Other Security Expert)*

> *'For outsourced security services, it is project driven. From a commercial point of view. Most of the time they are looking ..(for).. someone to stand at the gate or the door.'*
>
> *(Interviewee 5, Security Consultant)*

'In my experience where they do employ external contractors they take little interest in them – they treat them like a painter and decorator. The culture is such that they don't regard them much – not important enough … sets a spiral of downward culture.'

(Interviewee 13, Security Consultant)

The main difficulties for creating a good security culture

4.32. Given that there are many aspects to creating a good security culture, we asked interviewees to consider which elements pose the most difficulty.

4.33. A number of interviewees observed that creating a good culture was **generally a difficult** thing to do. It takes time to establish relationships and educate people, and is a continuous challenge:

'It is a massively difficult thing to do.'

(Interviewee 15, Security Consultant)

'I don't think there is generally enough awareness of what promotes or dilutes culture, we just don't go into it deep enough.'

(Interviewee 16, Security Consultant)

'Positive culture is important and not easy. It takes time. There is a skill to it.'

(Interviewee 18, Other Security Expert)

4.34. Although one interviewee felt otherwise:

'It is easy if it is something you want to do or understand the importance of. There is enough expertise out there and plenty of support which is accessible, so this is not a mystery.'

(Interviewee 20, Supplier – Senior Leadership)

4.35. In terms of the main difficulties, a number of themes were apparent. As may be expected, these generally corresponded with the issues identified by survey respondents but offered considerable further insight.

4.36. Interviewees commonly reflected that **not valuing** security, was a major barrier to a positive culture. Where organisations fail to see the value of security, indeed, where they see security as a separate function that someone else takes care of, or where they see security as a barrier to be overcome, there is no impetus for the workforce to contribute:

'Organisations that have a strong security culture have had success about communicating to leadership the value proposition.'

(Interviewee 6, Supplier – Senior Leadership)

'When you mop up after a major incident it's clear people haven't followed the rules and the bottom line is it's because they don't value security high enough.'

(Interviewee 13, Security Consultant)

'In the nuclear sector it is not a barrier because they see the significance but in commercial office space they see security as a barrier because challenging people walking around is viewed differently. If you want people to think differently then you need the business to recognise security as being important.'

(Interviewee 14, Supplier – Senior Leadership)

'People don't know what security is. Many talk about security people being business focussed but really the conversation should also be about business people becoming security focussed; they too often are not right now. Security is still not valued and utilised properly, there is still this view that security is just this person on reception.'

(Interviewee 18, Other Security Expert)

'Clients too often think I can pay someone to open the gate and if the organisation suffers damage that is the fault of security, there is so much tunnel vision and there is not appreciation of the security threat. We can do a good job but a better job with their help. It may cost them but they don't appear to worry about that.'

(Interviewee 19, Supplier – Security Manager)

4.37. One interviewee highlighted that there is **inherent difficulty** of showing the value of security:

'The perennial challenge with security is demonstrating value. We don't know the money we save from having a good culture. People who would steal from us, don't come and give us feedback and say we were going to try to take that but your security is too good so we decided to go down the road.'

(Interviewee 7, In-house Security Director)

4.38. And some lamented that there is still a need for **bad** things to happen, for organisations to listen to the advice they were given:

'The level of buy-in to [counter-terror training] ranged from disinterest to outright hostility. Post the Manchester arena attack, that attitude changed very quickly. It is sad to see it, but the easiest way to implement a security culture is something bad to happen. It's not the ideal answer. The ideal answer is we persuade them of the need prior.'

(Interviewee 9, In-house Security Director)

'The client ego when it comes to a lack of understanding of security. They are not seeing security as key. It is only

when something bad happens does security get a mention.'

(Interviewee 19, Supplier – Security Manager)

4.39. Some interviewees highlighted that a **negative perception** of security and security officers was still a significant barrier to organisations valuing security and ultimately to being able to generate a positive security culture:

'When we and others have led campaigns around a challenge culture it always seems to provoke controversy. There is something in the psyche that this is not at one with a good company culture, implying surveillance, that sort of thing.'

(Interviewee 22, Other Security Expert)

'I am doing a security strategy for a pub … they had four break ins and yet they have not installed any security and their culture is don't worry it won't happen again, and they are very relaxed, a lot are like this. They don't care about risk. The don't like security, it is bad for their reputation. So it may be worse getting burgled but they blame the lack of police and everyone but themselves.'

(Interviewee 17, Supplier – Security Manager)

'Security is often seen as a hurdle to people doing their work, but right from the start through induction, and appropriate delivery it can be an enabler and should be.'

(Interviewee 14, Supplier – Senior Leadership)

'There is also the stereotype too of security staff which is not complimentary, and we have to overcome that.'

(Interviewee 19, Supplier – Security Manager)

'We've had a real push – the long term unemployed to get them off the dole books are paid to get a badge then are in a frontline security role which they have no motivation to be in – they are there to avoid sanction or losing benefits. They are there begrudgingly because they would lose their home if they didn't do the security job. That doesn't set the right culture – it is seen as low paid, low skilled work and bringing people off the doll queue has exacerbated that view. Most of them lean against the thing, disinterested, disengaged – they don't want to be there. They are going through the motions. That as part of the security culture is wrong – you want the bright-eyed, bushy-tailed, the motivated, the interested, you want to support with ongoing development. You end up in a scenario where no one cares.

(Interviewee 4, Other Security Expert)

4.40. Indeed, one leader for a global security supplier company talked about how they sought to address the barrier to security culture posed by the negative perception of security officers by investing in their officers (for

example with additional training and quality uniforms) and deciding not to bid on minimum wage contracts:

> *'So we decided we would not bid on minimum wage, we had our own view on enhanced value so we changed the way officers were recruited, also we spent more on retention so they felt they had some investment. We invested in officers, and that matters for what stakeholders think as well as what officers think. [The officers] feel part of it. They are smart and engaged.'*
>
> *(Interviewee 21, Supplier – Senior Leadership)*

4.41. Linking to the points on value and perception of security, was the issue of investment. Some interviewees observed that security is **under-invested** in and consequently staff are low paid, equipment may not be upgraded and more generally a lack of investment can send a message that security is not prioritised which undermines any efforts to build a positive security culture:

> *'Budgets are a key point. That is key to a more effective culture – good wages, good training, consistent and good employment rights. People feel security is a must have rather than a positive asset. They use the cheapest, easiest staffing they can possibly have, then that effects the culture. Security in terms of wages hasn't really moved in 12 years. £15 per hour may have been reasonable 12 years ago. But now you could stack shelves in [a supermarket] for that. But you also have to pay for licences and travel, there is a lot to pay out.'*
>
> *(Interviewee 2, Contracted Operative)*

> *'In this industry where a lot of the staff are low paid it is utmost ensuring you have food on the table. Many do the job because they need to. The marketplace is full of people trying to get that extra pound or so.'*
>
> *(Interviewee 3, Supplier – Account Manager)*

> *'Financial pressure comes. Organisations start to ask, do we need as much security as we did. Maybe make cuts or not do planned upgrades. Or if you make a new acquisition you want to upgrade to the global standard but could that wait until next year. The danger is that if the business or people feel there isn't investment made in security, does that send an underlying message that we don't care about security as much as other things? If you don't handle that well that can impact culture.'*
>
> *(Interviewee 7, In-house Security Director)*

4.42. Another key theme, closely linked to the notion of value explored above, was whether security behaviours and attitudes and ultimately culture was **endorsed by the leadership** of the organisation. Interviewees often referred to the 'tone' being set at the 'top' and that a lack of senior level

buy-in was a major barrier because if they don't take security seriously, no one else will:

> *'The culture starts at the top. 99% of the time if it goes wrong, it's because the governance structure isn't right. There should be a board level, c-suite individual with named accountability for security. Only then have you got any chance whatsoever of enforcing security related matters.'*
>
> *(Interviewee 9, In-House Security Director)*

> *'So the clients and c suite of the buildings where I provide security, they are more reactive to security, it is not a practice that is their concern. With security culture, honestly, it sits on a shelf in a binder, honestly. Maybe it is getting better but what I see is written as compliance and seen as just that.'*
>
> *(Interviewee 19, Supplier – Security Manager)*

> *'It's like a fish – it starts to stink from the head down.'*
>
> *(Interviewee 10, Other Security Expert)*

> *'From the chief exec of an organisation right the way through. That has to be right to have any chance of delivering the culture at grass roots level. If the leader acts in a certain way, invariably that will percolate down.'*
>
> *(Interviewee 8, Supplier – Senior Leadership)*

> *'[In construction] there are some very senior people who have never had a day's education about their responsibility to protect; it is not part of their thinking. When I say you need to become the risk owner they say you are the security manager. I say no, I am the advisor on how to reduce risks. I am educating very senior people and it is wrong that they don't know. We need to build this knowledge into their early careers. We can't create a security culture if we do not.'*
>
> *(Interviewee 15, Supplier – Security Consultant)*

4.43. However, one interviewee observed culture may not need to be set from the top, as long as someone influential was championing it:

> *'It does not have to be driven by people at the top but there needs to be the right mindset generated by someone. I think it is easier that way but if the top person empowers others then it can be done.'*
>
> *(Interviewee 20, Supplier – Senior Leadership)*

4.44. Two interviewees talked about how the 'tone at the top' should **extend to the 'authorities'** working to ensure organisations prioritise security:

> *'There is not enough push back from the authorities. All [crime] damages our economy and is boosting the wrong people's finances. As a society we are poorer because thefts are being used to fund horrible things in our*

communities. The Police and Government need to do more to encourage organisations to develop better security cultures. Not a hashtag or a conference. This needs to be a continual development thing.'

(Interviewee 4, Other Security Expert)

'The issue is in terms of priority. Security is not a priority. It is not for Government either.'

(Interviewee 23, Other Security Expert)

4.45. **Communication** was another key theme raised by interviewees. A number of issues were apparent here. First, was the difficulty of **reaching** the whole of the workforce – ensuring that the security messages are heard and moreover prioritised, among a cacophony of other messages and other priorities:

'Partnership with internal communications teams around messaging. They will limit the amount of communication that can go out. They are worried about message burnout. Security is one voice of maybe 20 departments. That partnership is important to be successful.'

(Interviewee 6, Supplier – Senior Leadership)

'Also, one thing I do think – getting your message through in the noise of all the other business elements. The communication space is too cluttered. How does your message cut through – how do you make sure your message competes in that busy space for the employee.'

(Interviewee 11, In-house Security Director)

'Who will drive the communication and be responsible for the bulletins? You have to be en pointe otherwise people will ignore it. And [the message] has to be easy to follow.'

(Interviewee 24, Supplier – Senior Leadership)

4.46. Second was the challenge of turning information in to action. It was clear that it is not enough to communicate what to do; the workforce need to understand **why** and there needs to be a clear benefit:

'Linking it to the people and making it accessible. Showing that there is something in it for them. There has to be a visceral connection. It is not done by scaring people but by helping them understand.'

(Interviewee 6, Supplier – Senior Leadership)

'You need to think in terms of what they want, say you are thinking of protecting them, helping them to do their job. You can change attitudes but it takes time.'

(Interviewee 17, Supplier – Security Manager)

'Sometimes in organisations there is still a perception that security is something that is done to them. Sometimes the security communication is directional, giving orders. People don't warm to it or they think it's not relevant to me. The perception and buy-in of the workforce. You can show the leadership with metrics and information why they

should buy-in and they tend to do so. But the workforce. Being visible in and around the business space. Being one of the team. All in it together. You want to be in people's thoughts and minds more, not locked away, not self-isolated. Build trust and collaboration. That's a challenge.'

(Interviewee 11, In-house Security Director)

'Scaremongering or whipping up fear might generate an effect in the short term, but when the bad thing doesn't materialise people will start to test that. You have to get the right balance of genuine threat or concern, but not just bad things will happen so just comply.'

(Interviewee 7, In-House Security Director)

4.47. Third was that in order for people to continue to exhibit the right behaviours, there is a need to communicate that their efforts have been **worthwhile** and this is an ongoing process:

'Some security approaches don't help. They may have done some security awareness training, and the question is are they really engaging staff? Are they following up? Are they recognising people for doing the job well? It is a matter of a nudge rather than a stick.'

(Interviewee 18, Other Security Expert)

'Creating the right mindset. Make sure people are rewarded for 'see something say something' – get their reward – thank you. So they can recognise that whatever it is they see it could be significant, it could factor into something bigger.'

(Interviewee 12, Supplier – Senior Leadership)

4.48. In terms of how best to communicate, one in-house security director specifically observed that e-learning, rather than written messages had been successful for engaging the workforce:

'I find very short e-learns, animated e-learns are probably the most beneficial – 5 minutes, sort, concise and to the point. We've had really positive feedback. We focus on situational awareness – what to do if something bad happens, what you will feel, where to go for help.'

(Interviewee 1, In-house Security Director)

4.49. That individual had also found that educating people about the role of security and the largely unseen work of the security team was beneficial for engaging people with security:

'99% think it is just people on a door checking passes. So sometimes rather than making a point it is giving insights into what you do. It creates a bit more appetite through wanting to know what goes on.'

(Interviewee 1, In-house Security Director)

The impact of recent trends on security culture

4.50. Acknowledging that there have been many challenges in recent years that have impacted on organisations generally and security specifically, we asked interviewees whether they had observed any impacts on security culture arising from recent trends.

4.51. One interviewee (*16, Security Consultant*) felt that despite the number of 'big events' in recent times they didn't believe there was much impact on culture overall. And another noted that for security, events around the world are **par for the course**:

> *'They happen and will always happen. We deal with them as business as usual.'*
>
> *(Interviewee 1, In-house Security Director)*

4.52. On the other hand however, another interviewee (*11, In-house Security Director*) suggested that achieving a strong security culture would be **more challenging** in future as the security threats increase and become more complex.

Benefitting a security mindset

4.53. Some interviewees noted generally that recent events had helped to **raise the profile** of security. A 'crisis' can highlight the value of security and also gives security the chance to shine:

> *'I feel we are shifting a little bit in mentality. Covid has opened people up to the importance of safety and security. It only takes a global pandemic for people to notice.'*
>
> *(Interviewee 4, Other Security Expert)*

> *'I think that trend of resilience, dynamic agility is a definite positive that we've bounced from pandemic, to war – its shown the value of security in the broader enterprise risk sense.'*
>
> *(Interviewee 11, In-house Security Director)*

4.54. Some had seen this translate to **greater buy-in** at the senior level:

> *'I don't think there is anything like a crisis to drive a plan. I would say when there is a third of our clients asking us to activate our active shooter drills say, there is a trend in the industry where there is a reaction to a tragic event, you can see the reaction from corporate entities.'*
>
> *(Interviewee 24, Supplier – Senior Leadership)*

> *'I have worked in emergency planning for the last 4 years with the [health sector]. Previously the chances of getting senior management buy-in for emergency planning for a pandemic would have been non-existent. We would be fine now.'*
>
> *(Interviewee 9, In-house Security Director)*

'Historically organisations haven't wanted to hear the bad news. Leadership has resisted the message of 'the baby is ugly'. That has to change. How you communicate that message is going to be important.'

(Interviewee 6, Supplier – Senior Leadership)

4.55. Or among other departments such as Business Continuity Planning:

The one trend is to bring security and BCP closer together – a lot of those crises – travel crises, Ukraine crisis, and I've heard similar from others, had similar experience with our people – the ability of security to work in those ambiguous situations was a real benefit to BCP. Security people are used to that. I think that was really valuable in this unstable environment.

(Interviewee 11, In-house Security Director)

4.56. Although one interviewee observed that any benefits from events tended to be **short-lived**:

'Things boom when there is an incident, but things soon get forgotten when the media calms down.'

(Interviewee 19, Supplier – Security Manager)

4.57. Another interviewee suggested recent events highlighted the need to be prepared for a **wider range of issues**; a capability that they felt would result in security having greater influence:

'You will get tube strikes and you will get floods and there needs to be an assessment and getting these on the risk register. It needs to be a constant living document. It is just common sense. Good security is about being recognised as an expert and thereby having an influence.'

(Interviewee 18, Other Security Expert)

4.58. Some interviewees observed more specific examples that may benefit the security mindset.

4.59. One interviewee noted that **cyber issues** had raised the security mindset and that this awareness and understanding would also be beneficial for physical security:

'The online type stuff – cyber security, information security – has exploded over the last 10 years. So we have a generation that is au fait with online security which raises the security culture mindset. We use a lot of cyber culture – we piggy-back on that for the physical side and its stronger now. The younger generation understanding the need for security.'

(Interviewee 1, In-house Security Director)

4.60. Another noted the pandemic had created a focus on **compliance** with rules which made individuals more inclined to follow security requirements:

'Broadly speaking if anything and looking at the pandemic I do think that when it comes to people enforcing rules, people were more rule compliant. We had to be it was lockdown. So security sort of gained form that, security rules mattered for a while. It is good people are following rules. But not being allowed to question rules is a negative I suppose.'

(Interviewee 24, Supplier – Senior Leadership)

4.61. Another noted that **terrorism** was a significant concern among organisations and that this offered a reason to engage with security and build an effective culture:

'Terrorism exists and it focusses the minds of clients and so the officers have a great value. Where clients are committed to working with us our officers will be involved in a diverse range of activities that can be serious and important. It is easier to integrate and align and build cultures.'

(Interviewee 21, Supplier – Senior Leadership)

4.62. The prevalence of **protestors** was also flagged as a concern among organisations that created an interest in security and therefore an opportunity for engagement and to build a unified response:

'All the different types of interest groups. We have clients in the building that are very keen to ensure we are regularly briefing them on intel we receive about certain protestors and whether they are likely to stage a protest around the building.'

(Interviewee 3, Supplier – Account Manager)

Undermining a security mindset

4.63. There were three main recent trends that interviewees saw as potentially undermining a security mindset and therefore as important to address.

4.64. First, was the increased use of **working from home** that resulted largely from the lockdowns during the Covid-19 pandemic but has continued. A key concern was that this style of working created a more relaxed attitude and less possibility for oversight which can **raise the risks** to the security of employee devices and create specific opportunities for fraudsters to exploit:

'Working from home has undermined security at least. Within offices you have a bit of control. With 'hybrid' working or 'distributed' as some call it. The ethos is that everybody has to know everything – because they are working elsewhere, everyone has access to everything. They are just given access, so the security environment or control has – the digital world is fooling the senior directors,

managers in to thinking that security is taken care of. The CSO has assured them that yes, we've got that under control. Who do you believe the CSO on the board, or a minion of a [security] manager dealing with locks that is saying no – information is going out, it is not in the protected environment you think it is.'

(Interviewee 5, Security Consultant)

'Remote working has brought an increase in risk of cyber security breaches. It's about education. Lots about phishing emails and what not to open. I think further down the line we will see more outsourced penetration testing – ethical hackers – we are better off eating our own lunch before someone else does.'

(Interviewee 10, Other Security Expert)

'We've seen the impacts of fraudsters applying for remote jobs – equipment is sent to them, to the tune of 30 million dollars a month for one firm. Remote creates security challenges and how the security function addresses those is one challenge.'

(Interviewee 6, Supplier – Senior Leadership)

4.65. Indeed, one interviewee noted the imperative of physical and cyber security working together to create an effective security posture and build a security culture:

'The problems are less stove piped; they are now converged. It's become more critical for cyber and physical to work together because the threats converged, so organisations that failed to make progress on that front are less successful in managing the cultural and operational issues in that environment.'

(Interviewee 6, Supplier – Senior Leadership)

4.66. Interviewees also suggested that working from home has meant there is less opportunity for the workforce to see and therefore absorb the culture, and consequently there was some **skills fade** in the respect that employees forget security practices when they are not in the office using them regularly:

'When people were in the office more regularly lots of things happened by osmosis – using passes, the process for visitors. Now with working from home people have forgotten all those skills through the pandemic and not being in that routine – people just forget about it – just out of sight out of mind.'

(Interviewee 11, In-house Security Director)

'There is work to be done to raise security awareness around hybrid working. If they are not coming into the office, they may be more relaxed, not taking security so seriously. [We need to develop] the security envelope and advice we put around that. From a whole business cultural

point, being in the office, that is where you see and learn the culture. You can't understand culture if you are permanently on zoom calls.'

(Interviewee 1, In-house Security Director)

'Fire drills – previously at 2pm on a Thursday afternoon you would have caught 80-90% of the office population. Now that would be 10-15% of the population. So when a fire event happens, some people might have forgotten – that is a simple example but it highlights the challenge – spending less time in the office people are less aware of requirements, are they less able to respond to events? Not because of laziness or incompetence, just match fitness.'

(Interviewee 7, In-house Security Director)

'It is not just [working from] home but lots of places so it is even harder to drive a security culture. We are in transition and learning what this hybrid looks like. So far this has not matured; our ways of working we are still in the evolutionary phrase. A number of clients are identifying they have security culture challenges because of this but we don't have a fix yet and there is no one size fits all.'

(Interviewee 14, Supplier – Senior Leadership)

'Culture is one of the things that is impacted when people are working from home as the company is fragmented and it is difficult to build a culture of everyone working together at least it needs more work to achieve and some different tactics.'

(Interviewee 20, Supplier – Senior Leadership)

4.67. In a different way one interviewee talked about how security has a role to play in creating a positive rather than a negative environment that will encourage people back into the office and that this presents both an opportunity and a challenge:

'We are encouraging people to come back to the office, there needs to be a reason to come in. We can't have security being a negative experience. It has to complement that positive experience. There is a dilemma, you want to be positive, supportive and engaging, but by same token you want people to remember the basics.'

(Interviewee 11, In-house Security Director)

4.68. The second main concern interviewees held was that current **financial trends** were impacting negatively on the security mindset. Primary among these, was that financial pressures leads to organisations **reducing their spend** on security which can reduce the quality of security and compromise the culture and mindset:

'Recently, organisations share prices were impacted, because of finance challenges in the US which came over here. That will focus some organisations on trying to reduce costs. Likewise the increase in energy costs will put

pressures on supply chain costs. So even good, focused organisations – there could be challenges in reducing spend in all areas. Security is often seen as the first cut that is looked at.'

(Interviewee 8, Supplier – Senior Leadership)

'Cost of living matters here and the pressures people face, not least in security where people are on low wages. Also there is the notion out there about the scarceness of security, they can't find staff or retain staff, numerically there are more than ever, but post covid resources have been taken away, [Supermarkets] offers a better deal to many.'

(Interviewee 23, Other Security Expert)

'When there is less money there are less resources, and people have a mindset as to where to spend the restricted resources and security is less likely to feature, and clients won't try new things as much, or not where there are costs in doing so.'

(Interviewee 20, Supplier – Senior Leadership)

4.69. Further, one interviewee warned that 'penny pinching' on security was a false economy that can end up costing more in the longer term:

'The cost against value debate has always been present but is much more prevalent now. Procurement know the cost of everything and the value of nothing, it is harsh but fact. They penny pinch to save a pound but underestimate the value of what is being offered. What frustrates me, is they penny pinch now and when expectations are compromised which they inevitably are, then suddenly it costs a fortune to put right, costs that would have been a fraction had it been done correctly in the first place. They spend money the wrong way around.'

(Interviewee 14, Supplier – Senior Leadership)

4.70. There was also concern that current financial challenges have been increasing the **violence and abuse** experienced by the workforce including security officers and that where this occurs it undermines a positive security culture because staff do not feel protected:

'The downturn causes struggles, and then there is more violence at work and it is continuing and people are stealing more over the need for money. None of this helps create a positive culture which also creates an adverse attitude to risk.'

(Interviewee 15, Security Consultant)

'The cost of living in the retail sector is having an impact on the amount of abuse retail workers are getting – we are starting to see more people sit up and pay attention to that. We are shifting a bit in our mentality towards that security culture but we still have a long way to go.'

(Interviewee 4, Other Security Expert)

4.71. Similarly, there was also concern that financial pressure was leading to more **temptation** towards dishonesty and crime:

> *'Seeing hyper-inflation at the start globally, so financial pressures will increase and cause people to be more tempted – how do we take that temptation away – get into that carrot and stick again – financial pressures tenfold compared to what they were a few years ago. Some things are in short supply – money doesn't keep everyone honest (reimbursement for work) – sometimes causes them to be dishonest – goes back to leadership are they active honest leaders?'*
>
> *(Interviewee 12, Supplier – Senior Leadership)*

> *'The economy is the fundamental driver. We may see more crime, some police think we will. The police are unlikely to get more funding, so there is a gap.'*
>
> *(Interviewee 22, Other Security Expert)*

4.72. The third main trend that interviewees felt may undermine a security mindset, was a number of recent **social movements** that they observed have led to a general **reduction in respect for authority**, and by extension security and further that such disruptions and distractions work against a positive culture:

> *'You also have the social movements. Views on authority have changed – police and authority. It impacts negatively on security and the police. It has changed the public view. It also makes it less appealing for people to want to join the industry and therefore weakens the culture.'*
>
> *(Interviewee 2, Contracted Security Operative)*

> *'… polarity doesn't help to bring people together with a security culture. Protests – counter protests against vaccines and isolation started a new kind of social activism that had been dormant for a long time – woke movement very much so – can see a backlash coming.'*
>
> *(Interviewee 12, Supplier – Senior Leadership)*

> *'Black Lives Matter and other social media induced initiatives are causing people to stand up more and to go against the leadership, it can be good of course but for me wanting a safe and security aware workforce these trends are bad. To be clear, for the individual oppressed by a leadership regime, that is [a good thing]. All these are disruptions to the workplace which complicate the process of creating cultures.'*
>
> *(Interviewee 15, Security Consultant)*

Future trends

4.73. Some interviewees commented upon other trends that may have an impact for security culture in the future. While the impacts were not yet

known, it was typically thought that these would be positive if managed well. This included the use of **Artificial Intelligence** (AI) in security technology, the introduction of '**Martyn's Law**' in the UK (which in short is due to be introduced to require certain venues to mitigate the terrorist threat), and considerations for **sustainable** practices and technologies in respect of security provision.

4.74. The next section of the report considers the implications of the findings from the surveys and interviews.

Section 5. Discussion and Summary Comments

5.1. In this section we attempt to highlight some of the key findings and seek to interpret them in terms of the aims of the study, and specifically what we learn about security culture. There are six key points.

5.2. First, security culture is linked to effective security. Survey respondents noted that factors such as effective security leadership, clear security objectives, an effective strategy and a strong security culture are important in delivering a successful security operation.

5.3. Indeed, and a second point, security culture is not just important, respondents felt it to be at least as important as strategy. After all, 6 in 10 survey respondents viewed security culture as important as security strategy, and more than 3 in 10 viewed culture as 'more' important than strategy, and in-house security leads (buyers of security) were especially likely to view security culture as 'more' important, well over a half did so.

5.4. Third, given this it will be viewed as disappointing that approaches closely linked to facilitating a security culture were often not commonplace. True, of the options explored a view that specified approaches 'never' take place was very rare, but they are certainly not universal. The findings suggest there is considerable room for improvement in terms of engaging employees with security behaviours and attitudes.

5.5. Fourth, impediments include organisational leaders not appreciating the value of security and not endorsing good practice, and a contributory problem of workers not engaging either. Somewhat ironically, this underlines the importance of strategy, and having aligned goals, and it also stresses the importance of the organisational culture being linked to the security culture. While not all thought it was essential our interviewees certainly stressed the advantages of the two being aligned.

5.6. Fifth, much of the literature on security culture has tended to stress the role of security as a protector, rather than as a business enabler, as a contributor not just to keeping assets secure but also helping the organisation to trade and make profits even in, and perhaps especially in adverse climates. Such a transition, one the security world has been keen to promote, brings with it changes in the requirements of a security culture. It is a moot point, as we found, as to whether broader engagement is needed to ensure protection (most thought it was), but it becomes all the more essential if security is to play a key role in helping organisations achieve their objectives.

5.7. A sixth point is that security is not just fighting its traditional Achilles Heel of underselling itself, it is also facing another one, failing to persuade its own (typically lower level) operatives that creating a security culture is

important or that it is good at it. While a large majority of respondents considered security management to be positive ambassadors they considered them less effective at communicating with the wider workforce to implement security requirements. Other notable impediments were: a lack of financial investment impacting on the quality of security staff engaged and high turnover and dissatisfaction; negative perceptions of security including some viewing it as an impediment to workers being able to do their job well; a linked point about a complacency with respect to security requirements; and sometimes fed by poor communication. Recent trends that may be impacting on security culture represented some familiar challenges (such as financial issues) but also some new ones (such as working from home) which serve to illustrate the point that security culture will need to continue to evolve - there is no room for complacency.

5.8. It is worth noting that a growing cyber threat in business, is that offenders are not just hacking in, they are logging in, facilitated by a lack of staff diligence or malfeasance. Creating a strong security culture is a main remedy to this type of threat, not just because it 'protects', but also because it enables ongoing business operations. There is a developing skill set – a discussion of which is way beyond the scope of this project - which emphasises the importance of communication in helping workers to understand the problem and see it as their responsibility to act, then feeling empowered to do so, and recognising the importance of it to do it well. A good security culture, protection and facilitating operations (and profit) are entwined and that link has not been universally recognised until now.

5.9. In short, a strong security culture is at least as important in achieving excellence as a strong strategy, but the reality is that both are required components of excellent security provision; neither is an option. What is clear though – from our survey respondents - is that this essential requirement is not widely understood, promulgated and certainly not always practiced. There is nothing new in us stating that security undersells itself, that it too often fails to successfully articulate its broader role to benefit the whole business, that all employees and stakeholders are potentially ambassadors for good security and potential weak links that can create vulnerabilities, so in a similar way are all processes. Understanding the whole business, all roles and the potential for each and every one to benefit security, and not the opposite, is a dynamic requirement. The key to doing this well is having a well-articulated strategy setting out a direction matched by a security culture that is conducive to achieving it. There is no short cut, as far as security is concerned strategy and culture are bedfellows, one without the other compromises performance. Now the security sector needs to articulate this and become very good at it, as many of those who work in security say there is enormous scope for improvement.

Appendix 1. Methodology and Sample

The approach

The study involved a review of available sources on security culture. These were used to give context and to help identify key issues and themes to explore in the consultation with security professionals.

The review of the literature was followed by two main approaches: 1) an online survey on security professional views on security culture; and 2) extensive discussions including semi-structured interviews with a range of security professionals to gain a more in-depth understanding of the topic.

Survey

The survey examined the views of security professionals on a number of key themes: the role of security culture in delivering successful security operations; the significance of culture; the level of engagement of the workforce with security; factors that support and impede a strong security culture; the impact recent trends have had on security culture; barriers to achieving a positive security culture.

The sample was, self-recruited and clearly those with an interest in the topic were most likely to respond. While no claims are made that the survey is representative of the security industry as a whole, responses were received from a range of roles and countries. Attempts were made to publicise the survey widely, including via participants from previous research who had elected to be contacted for future research; links in the Perpetuity newsletter and social media; security associations; security press; announcements made at conferences and other security events; and personal contact with a range of organisations who were informed about the survey and invited to publicise it and pass on the details to their members. We cannot be sure of the manner in which adverts were disseminated by these groups, but their contribution greatly enhanced the reach of our survey.

The survey ran from Friday 3rd February to Friday 17th March 2023.

A total of 258 responses were received, although not every respondent completed every question in the survey. The data was analysed using SPSS. The data are categorical; therefore, it is not possible to assess the normality of data. It is important that this is borne in mind.

One to one interviews

The approach in this work was to engage with security professionals from a range of roles and sectors that may be able to add insight. We engaged both informally and formally with a wide range of professionals in conversations about the issues covered in this report. This included during our series of

webinars on security.[40] We contacted specific people by word-of-mouth, and they sometimes referred us to others. We drew upon personal contacts and their networks; and some individuals who volunteered to offer more details after taking part in the survey.

Obtaining the sample in this way allows for potentially more valuable responses, as those taking part are more likely to be knowledgeable about the research. The interviews typically lasted thirty minutes and semi-structured interview schedules were used. The schedules were based on the information taken from the literature review as well as previous research. An advantage of a semi-structured schedule is that it gives the flexibility for interviewers to probe the issues raised.

We formally interviewed 24 professionals.

[40] Please see the OSPAs Thought Leadership Webinars – recordings are available here: https://www.youtube.com/channel/UC3ZsgjtdPBgJzs5yVzT-Lgw/videos

Appendix 2. Additional Data Tables

Table 2: Length of time respondents have worked in security (n=257)

Length of time	N	%
Less than 12 months	3	1
1-3 years	12	5
4-10 years	38	15
11-19 years	65	25
20-29 years	67	26
30 years or over	72	28

Table 3: Sector that respondents provide security in (all that apply) (n=258)

Sector	N	%
Public Admin, Other Services, Government	86	33
Retail	82	32
Property	81	31
Education	64	25
Manufacturing	60	23
Finance	58	22
Transport	58	22
Health	50	19
Energy	48	19
Leisure & the Night Time Economy	48	19
Other	48	19
Construction	47	18
Pharmaceutical	40	16
Production	36	14
Hotel & Catering	33	13
Post & Telecommunications	31	12
ICT	29	11
Mining, Quarrying & Utilities	20	8
Wholesale	18	7
Motor Trades	17	7
Agriculture	13	5

Table 4: Country where the respondent conducts the majority of their work (where they are based) (n=237)

Country	N	%
UK	171	72.2
USA	12	5.1
Canada	9	3.8
Ireland	6	2.5
Australia	4	1.7
Kenya	3	1.3
Iraq	2	0.8
Netherlands	2	0.8
Nigeria	2	0.8
Singapore	2	0.8
Sweden	2	0.8
Thailand	2	0.8
Zimbabwe	2	0.8
India	1	0.4
Switzerland	1	0.4
China	1	0.4
Austria	1	0.4
Bahamas	1	0.4
Bahrain	1	0.4
Belgium	1	0.4
Botswana	1	0.4
Finland	1	0.4
Ghana	1	0.4
Indonesia	1	0.4
Kuwait	1	0.4
Malaysia	1	0.4
Norway	1	0.4
Romania	1	0.4
Serbia	1	0.4
South Africa	1	0.4
Spain	1	0.4

About Perpetuity Research

Perpetuity Research is a leading research company with wide expertise in both quantitative and qualitative approaches. We have been extensively involved in evaluating 'what works' (and what does not). Our work has involved helping our clients to understand people's behaviours, perceptions and levels of awareness and in identifying important trends. Our mission statement is 'committed to making a difference', and much of our work has a practical application in terms of informing decision-making and policy formulation.
We work closely with our clients. This includes businesses, national and local governments, associations and international organisations as well as charities and foundations. Our aim is to exceed their expectations and it speaks volumes that so many have chosen to work with us repeatedly over many years.

About the SRI

The Security Research Initiative (SRI) started 19 years ago. It involves a rolling program of research; each year a separate study is conducted on the security sector to generate new insights, help develop the response and role of security and act as a guide to improving practice. The SRI is supported by ADS, ASIS International (UK Chapter), the British Security Industry Association, IFPO UK, IPSA, The SASIG, and the Security Institute, and includes membership from leading security suppliers and corporate security departments who share the commitment to the development of new knowledge.

Previous studies have focused, for example, on police views on private security; tackling cyber crime – the role of private security; the broader benefits of security; aspiring to excellence; the relative benefits and drawbacks of buying security as a single service or as part of a bundle; an industry wide survey; a study of the value of security. We have developed two toolkits, including one on developing a security strategy. The findings from the research are made available free of charge to all. More information on the SRI is available at: www.perpetuityresearch.com/security-research-initiative/

Perpetuity Research & Consultancy International Ltd
11a High Street
Tunbridge Wells
TN1 1UL
United Kingdom
Tel: +44 (0)1892 538690
www.perpetuityresearch.com
prci@perpetuityresearch.com

