Cyber Security Culture in organisations

NOVEMBER 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For media enquires about this paper, please use press@enisa.europa.eu.

ISBN 978-92-9204-245-5 DOI 10.2824/10543

Table of Contents

Executive Summary

The concept of Cybersecurity Culture (CSC) refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people's behaviour with information technologies. CSC encompasses familiar topics including cybersecurity awareness and information security frameworks but is broader in both scope and application, being concerned with making information security considerations an integral part of an employee's job, habits and conduct, embedding them in their day-to-day actions.

To assist in promoting both the understanding and uptake of CSC programmes within organisations, this report draws from multiple disciplines, including organisational sciences, psychology, law and cybersecurity. It is complemented by knowledge and experiences gathered from existing CSC programmes implemented within organisations, and contains good practices, methodological tools and step-by-step guidance for those seeking to commence or enhance their organisation's own Cybersecurity Culture programme.

There are multiple drivers behind the rise of CSC as a recognised need within organisations. It reflects the acceptance that how an organisation behaves is dependent on the shared beliefs, values and actions of its employees, and that this includes their attitudes towards cybersecurity. There is the recognition that cyber threat awareness raising campaigns are not, in themselves, affording sufficient protection against ever evolving cyber attacks. There is also the recognition that technical cyber security measures do not exist in a vacuum, and need to operate in harmony with other business processes to avoid that employees are placed in the untenable position of being forced to choose between 'doing their job' or 'complying with security policies'. Finally, it is about responding to the view that humans represent the weakest link in cyber security chains, and replacing this with an environment where employees become robust human firewalls against cyber attacks.

It is against this backdrop that ENISA has undertaken research into Cybersecurity Culture to provide this guidance, applicable to organisations regardless of structure, size or industry. This is achieved by presenting tools and practices designed to be contextualised to the needs and circumstances of individual organisations. While it has been targeted at those employed in security functions and/or tasked within increasing the cyber security resilience threshold of all employees, the language has been crafted to ensure all employees, regardless of role or seniority, can gain sufficient understanding of what is required to produce and kick-start their own CSC programme. The following resources have been included:

- Good practices identified from those organisations that have already implemented mature CSC programmes, and specifically categorised and tailored to different audiences within an organisation, from senior management to the information security team;
- To facilitate the development and delivery of a Cybersecurity Culture programme, an eight-step Implementation Framework is presented alongside detailed guidance for each of the constituent steps. This Framework encompasses the entire lifecycle of an organisation's Cybersecurity Culture programmes.
- Methods to produce a CSC for an organisation, as well as guidance on suitable metrics for measuring the impact of CSC activities; and
- Strategies for building a robust business case for the allocation of internal resources towards future Cybersecurity Culture activities.

The study will identify good practices, methodological tools and step by step guidance for those seeking to commence or enhance their organizations own Cybersecurity Culture programme, including resources to

produce a business case to secure funding for such a programme. The success of a CSC programme rests on a number of key elements, these elements are identified and described below.

Recommendations for a successful CSC programme:

1. Secure buy-in at the highest level

Senior buy-in at the highest organizational level is essential for the success of the programme. Senior figures are needed that can to act as champions for the programme and lead by example thereby influencing the staff's behaviour towards the programme.

2. Follow the CSC Framework for the implementation of the programme

The CSC Framework presented in this report provides a process to guide the CSC programme in the form of a step by step implementation centred around specific activities, their implementation and measurement of impact.

3. Know your organization so as to ensure success

This step within the CSC Framework is key to ensuring the success of the programme, because it will inform the decision making processes that define the goals, success criteria and target audience of the CSC programme.

4. Measure the current cybersecurity level of the target audience

Calculating the current level of CSC of your target audience will assist in measuring the effect of the activities you chose to implement and thus the impact of the CSC programme.

5. Draw upon the good practices identified in this report

A number of good practices have been identified from interviews with CSC professionals within organizations across Europe and desktop research that will assist in planning and executing a successful CSC programme.

1. Understanding cybersecurity culture

As businesses and individuals embrace technologies in their everyday activities, software and technical solutions that try to protect us from cybersecurity threats have multiplied. Yet, despite awareness of cyber threats, advancements in cybersecurity technologies, and an increased number of national and organisational **computer security incident response team** (**CSIRT**).to coordinate responses, both the frequency and costs of data breaches continue to rise. Humans remain the weakest link in the security chain, and investing in and developing cybersecurity cultures within organisations can decrease the human factor risk, imparting a positive impact on efficiencies and security while mitigating financial risks.

1.1 Scope of this report

This report is targeted at senior management to provide guidance and tools to affect culture change within their organisation by establishing and running of an internal CSC programme. The Step-by-Step Framework presented in Section 4 is designed to be applied and contextualised to the needs of any organisation that is seeking to develop a CSC programme, regardless of the organisations size, sector or structure.

1.2 Definition

Cybersecurity Culture (CSC) of organizations refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies. CSC is about making information security considerations an integral part of an employee's job, habits and conduct, embedding them in their day-to-day actions. Adopting the right approach to information security enables a resilient CSC to develop naturally from the behaviours and attitudes of employees towards information assets at work,[1] and as part of a company's wider organisational culture, its CSC can be shaped, directed and transformed.[2] However, business environments constantly change, hence organisations must actively maintain and adapt their CSC in response to new technologies and threats, as well as their changing goals, processes and structures. A successful CSC shapes the security thinking of all staff (including the security team), improving resilience against all cyber threats, especially when initiated through social engineering,[3] while avoiding imposing burdensome security steps that prevent staff from effectively performing their key business functions.[4]

1.3 The need for cybersecurity culture

The majority of data breaches within organisations are the result of human actors,[5] and while cybersecurity policies are commonplace among organisations, employees may view them as guidelines rather than rules. Similarly, technologies cannot protect organisations if incorrectly integrated and utilised.[6] Against this backdrop, the development of a CSC achieves a change in mindset, fosters security awareness and risk perception and maintains a close organisational culture, rather than attempting to coerce secure behaviour. In the upcoming sections, the different aspects of developing a CSC will be examined.

---

[1] Martins, A., Eloff, Jan, Information Security Culture (2002), p. 204-206.
[2] S. J. Ross and R. Masters, Creating a Culture of Security. 2011. L. Ngo, "IT Security Culture Transition Process," 2008.
[3] 2011 – McKinsey – Meeting the Cybersecurity Challenge, p. 3.
[4] G.V. Post, A. Kagan., Evaluating information security trade-offs: restricting access can interfere with user tasks, Computers & Security 26 (3) (2007).
[5] Ponemon Institute, 2012. The human factor in data protection [online]. Ponemon Institute.
[6] A. Fagerström, "Creating, Maintaining and Managing an Information Security Culture.," 2013.

2. Building a business case for implementing a CSC programme

This section presents strategies for those who wish to initiate a CSC programme within their organisation and need to produce a business case to secure resources for this programme. With different departments and initiatives within an organisation all competing to access a finite pool of financial and human resources, those seeking to implement a CSC programme will often have to produce a business case to justify the allocation of resources. To assist in this process by strengthening a CSC business case, we have identified and presented three sources of evidence that can incorporated. These being:

a) Wider sector-based statistics on current cyber threats
b) Evidence drawn from your cyber security team
c) Self-collected results of a pilot CSC intervention

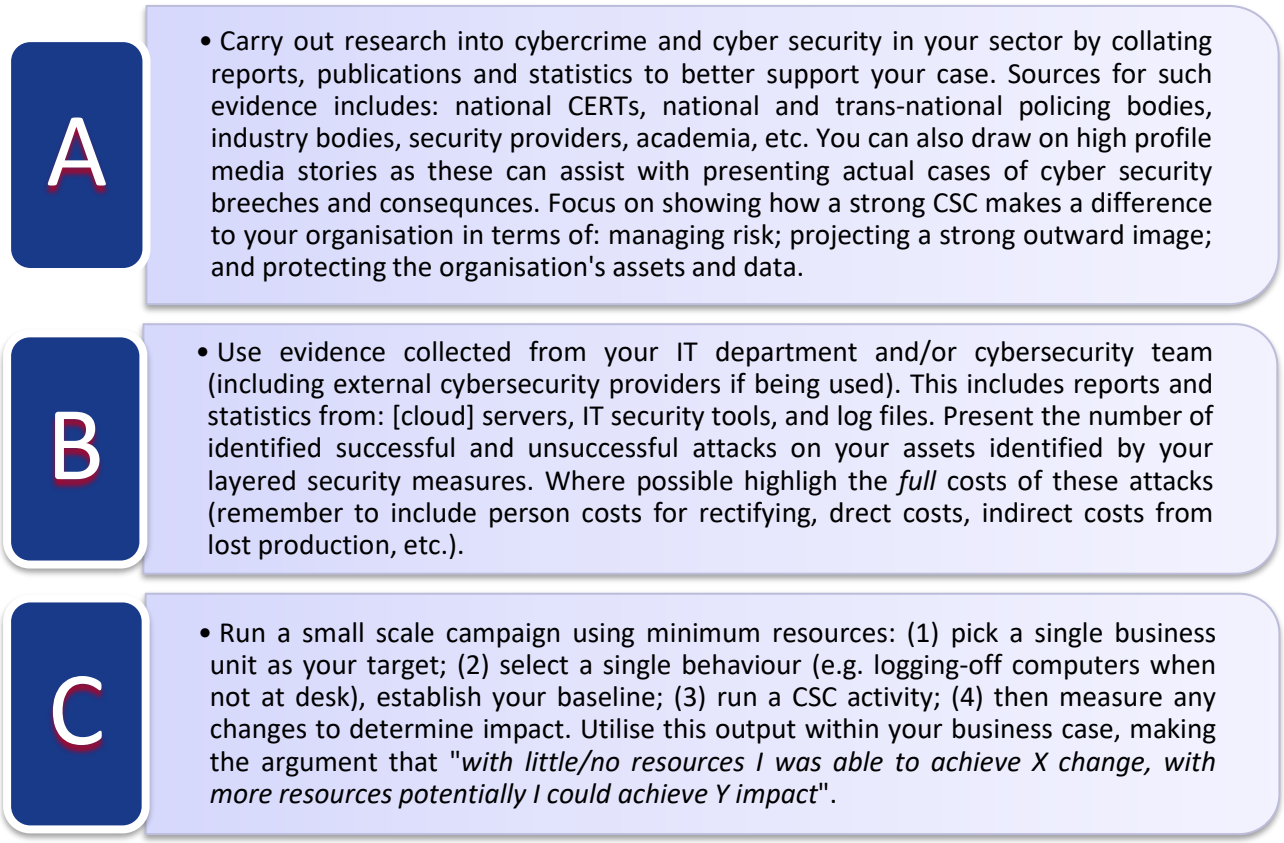

Figure 12: Three approaches to developing a business case for CSC

Whether you include one, more, and/or additional strategies within your business case will depend on the context of your own organisation. Factors to consider here include: how such cases are normally presented and processed within your organisation; the overall availability of resources within your organisation; and the importance assigned to cybersecurity. If the challenge of acquiring resources within your organisation is great, you may wish to include all of the approaches set out above. IF CS is already on the agenda, you may feel that a softer approach will suffice and thus you can choose which approach to follow. Decisions here will also depend on your resources (financial and time) and access to data.

3. Developing and implementing a successful CSC programme

Developing and implementing a successful CSC programme within organisations is a task that requires a multi-pronged and nuanced approach, involving senior management as well as other employees. Culture extends beyond awareness to include the shaping of beliefs, norms, values. It requires a mutual understanding between senior management, CS implementers and employees on what their roles, responsibilities and practices entail with regard to defending against cyber-crime.

Culture is also unique to each organisation, and to create a robust and sustainable CSC requires an in-depth knowledge of the organisation, its overall culture, strategies, policies, employee practices and processes. To be successful, a CSC needs to be embedded in the organisational culture and it should take into account employee needs and practices. If CSC programmes and activities become too burdensome, there is a risk of employees resisting or ignoring CS messages, technologies and practices being implemented. CSC must be formed *with* employees, rather than *imposed* upon them. That said, there is also a clear need for visible and vocal buy-in from senior management to provide legitimacy to, and a clear signal on the importance of, an organisation's CSC programme.

This section is dedicated to providing practical guidance to those seeking to establish a robust CSC within their organisation. This guidance draws on existing cybersecurity and CSC literature and guidance, as well as knowledge and good practices drawn from our consultation with both CSC experts and employees with CSC responsibilities within different organisations in Europe.

In developing this guidance, ENISA recognises the inherent challenge of providing a single set of prescriptive rules with relevance to all organisations, regardless of their size, sector, existing culture and/or location. There is no 'one-size-fits-all' approach when it comes to the most effective content and delivery methods for implementing CSC programmes within organisations. As a result, except for the Implementation Framework in Section 11, all the guidance presented below is specifically designed to be adaptable to the unique contextual needs of every organisation that employs it. Therefore, alongside the Implementation Framework, we provide optional components for creating, delivering, and measuring the success of, your CSC programmes, that are be selected and combined by the internal CSC implementation team based on their unmatched knowledge of their own organisation.

In Section 11 we provide a step by step framework/guide for setting up your CSC programme and explain how to assemble the strongest possible CSC working team. Again, this will differ within each organisation, but the focus provided is on the necessary capacity for each member so if your organisation hierarchy is different, it is clear which members you need to drive the implementation forward.

Section 12 provides a guide on how to create a receptive environment within your organisation, which is imperative when it comes to delivering your CSC messages and training. In Section 13 we provide list of CSC activities, as well as providing two methods for constructing the current level of CSC before starting any activity, so that any change in culture can be accurately measured. We also identify and present good practice metrics, that will allow you to monitor this behavioural and cultural change. In Section 14 we provide guidance on how to build a strong business case for CSC to ensure support from senior management and Section 15 presents identified good practice in building a strong CSC within organisations.

4. An implementation guide for CSC programmes

This section provides a process covering the creation and implementation of CSC programmes in the form of a step-by-step Implementation Framework centred around specific activities, their implementation and measurement of impact. The approach is iterative in that after each CS activity is run, impact is measured, results considered and the approach is reviewed. Following this, new activities may be chosen, or delivery methods may be changed. This also gives an opportunity to consider and amend initial goals and/or the target audience. A detailed description of each step is provided in Section 12.1.

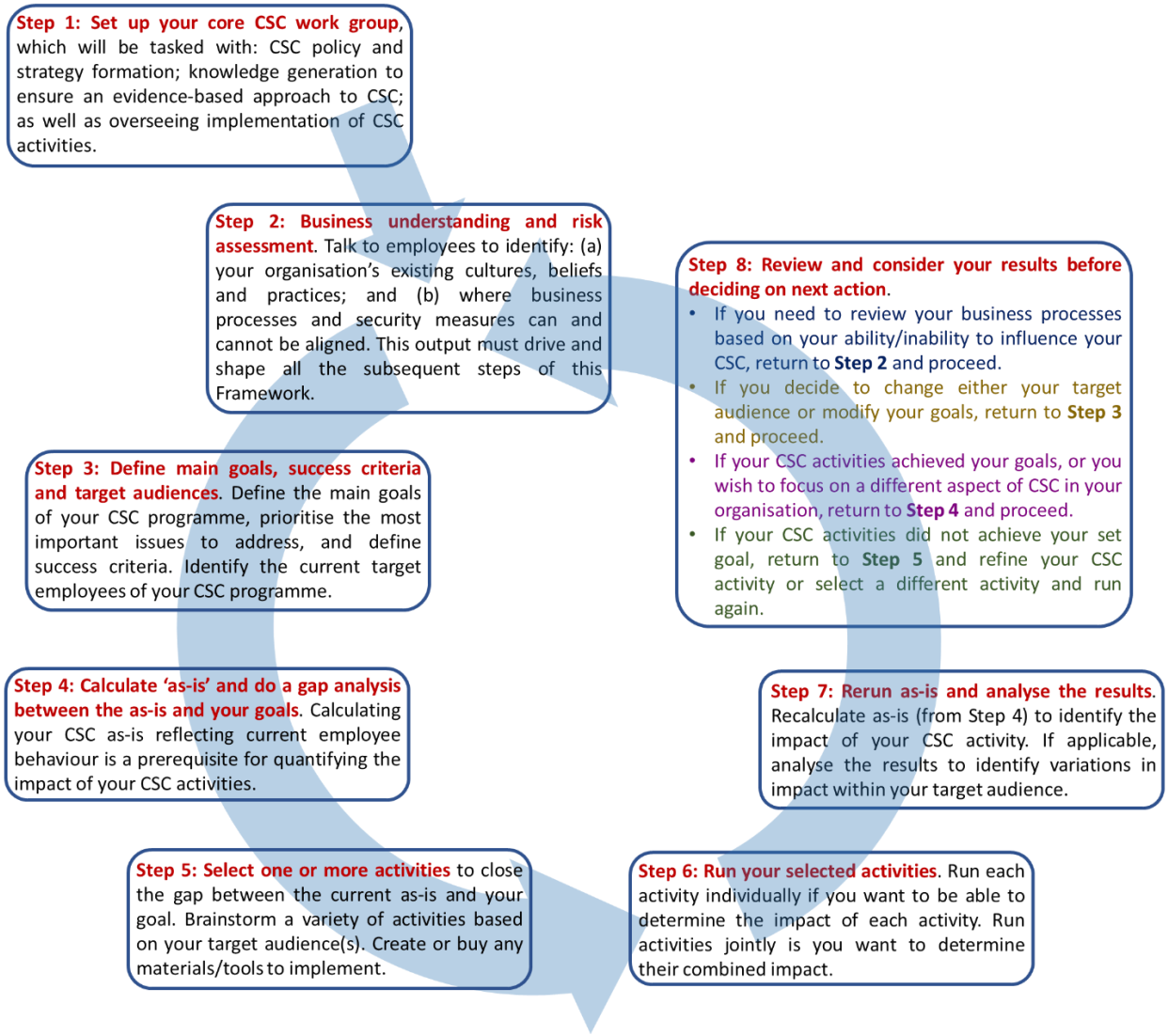

Figure 7: Step-by-step framework for organisations to implement a CSC programme[7]

[7] The structure for this framework is grounded on The Security Culture Framework developed by Kai Roer, incorporating the feedback of interviewees collected during the course of developing this guidance.

While each organisation may need to modify the Implementation Framework to meet the unique needs of their context, such modifications should be undertaken with care. If changes are required, we strongly recommend the following guidance is followed:

a) The insertion of any additional steps and/or processes to meet bespoke needs of the implementing organisation is encouraged providing they do not undermine the existing steps.
b) Apart from switching the order of Steps 1 and 2, we strongly advise against any other modifications to the current ordering.
c) Do not be tempted to skip or remove any of the existing eight steps. Each of these steps serves a specific purpose in developing a robust CSC programme.

4.1 Step-by-step plan for implementing a CSC programme

Provided below is detailed information for each of the eight steps integrated into Figure 7. As per Figure 7, this process is iterative/circular in nature, rather than strictly linear. You circle back to earlier Steps in the process when: refining CSC activities; selecting new activities; selecting new elements of your organisation's CSC to address; selecting new target employees as the focus for CSC activities; and modifying your goals. These possibilities are visualised in Figure 7.

Step 1: Set up your core CSC work group

This group will be tasked with knowledge generation to ensure an evidence-based approach to CS, as well as formation of the CSC programme and strategy, overseeing the implementation of CSC activities, and ensuring alignment with the organisation's cyber security policy. Bringing together a core team from five specific areas within an organisation maximises the potential for future success of that organisation's CSC programme. This core team also requires the support of senior management to champion the CSC programme. Membership of the core team is set out in Figure 8 below. In addition, additional representatives from the wider organisation may also be included, depending on the contextual nature of the organisation at hand. Details on the knowledge and expertise that each member of the core team contributes to the wider CSC work group is presented in Section 12.2.

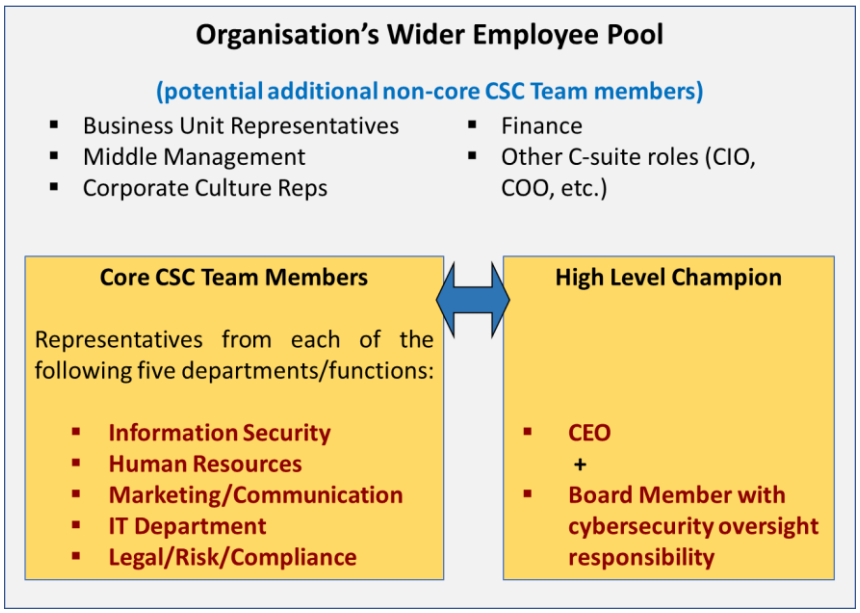

Figure 8: Core and non-core members of a CSC working group

Step 2: Business understanding and risk assessment

This step involves understanding what values, cultures, beliefs and practices already exist within your organisation and why they are there. This knowledge is likely available within each department and team. It is important to look at the different needs of each team/department and specific job roles as these may differ quite substantially and there might be barriers to success that you will be unaware of unless you consult with employees.

An essential element in this process in *understanding your business* is mapping and assessing the current/future security measures implemented by the security team against the processes that must be undertaken within each business unit if those employees are to fulfil the requirements of their roles. This mapping and comparison of business process against security measures will enable the CSC team to identify where:

a) *synergy exists* between business function and security measures – whereby security measures do not prevent or negatively impact the execution of business functions;
b) *compromises exist*, where security measures negatively impact business function, however, through some modification on either/both side a solution can be reached that is acceptable to both sides;
c) *conflicts exist*, where security measures and business functions cannot co-exist as one prevents the other.

In the case of (a) and (b), achieving compliance with cybersecurity practices in a collaborative manner will be achievable. However, in the case of (c) the organisation will need to undertake risk assessment and cost-benefit analysis to determine whether to abandon the security measure and accept or address the risk is some other way, or to abandon the business practice if the security risk is considered too high. This represents a business decision and may need to be escalated to the organisations *Risk Committee*.

This mapping process to identify synergies, compromises and conflicts, is fundamental to the success or failure of any future CSC programme. If employees are placed in the position of not being able to do their jobs without breaking cybersecurity rules/policies, then the CSC within that organisation is likely to become toxic and resistant to change via any subsequent CSC programme. This mapping process also fosters two-way engagement between the security/IT team and profit-centres/business-units, enabling both sides to better understand the needs of the other, while identifying issues requiring strategic decisions and ownership by senior management. Your CSC helps protect your organisation, thus, when developing your CSC activities, it is important to know what assets cyber criminals are likely to seek out. For example, if you hold a lot of valuable data, you need to focus on this specifically, this will involve in-depth understanding of your current data collection, processing and storage facilities, the work processes around data, physical location of servers etc.

Your CSC needs to align with your current organisational culture and avoid amplifying any weaknesses. Thus, it is important to critically examine the current culture with regard to strengths and weaknesses so these can be taken into account. Culture is dependent on context and is composite of people, communication, practices and location. You need to talk to employees and find out about their day–to-day work and how CS can fit within their activities. If CS is perceived as a burden or obstacle, it will likely be ignored by staff.

Step 3: Define main goals, success criteria and target audiences

For each organisation, it is important to clearly define the main goals, and the associated success criteria for judging when these goals are met, in relation to your organisation's future CSC. When doing so, recognise that some of these goals will have universal application across the entire organisation, while others will be targeted at specific groups/roles. This process of defining goals and the associated success criteria, will assist with calculating your current CSC situation and defining metrics in Step 4. Also, define your target group(s)

(e.g., everyone or specific department). For larger organisations who are starting the development of a CSC it might be beneficial to start by focusing on a specific target audience, before broadening out to include all members of staff.

Step 4: Calculate the current situation and do a gap analysis between the current situation and your goals
You cannot quantify the impact of your future CSC programmes if you do not first establish the current sitiation (as-is) that represents the current CSC level of your target. Hence, here you calculate the current situation and do a gap analysis between the current situation and your goal(s). There are three main approaches (each discussed in detail in Section 13.2, including their advantages and disadvantages to assist in your selection process):

1) Determine your CSC current situation independently from your CSC interventions
2) Determine your CSC current situation by utilising your CSC intervention metrics
3) Combine approaches 1 and 2

Placing this Step in the wider process under this framework, the plan is to create the current situation in this Step, then select and run your CSC activities in Steps 5 & 6, before re-calculating the current situation in Step 7. Following this process will also allow you to measure the effect of the activities you choose to implement. For more details on metrics and current situation calculation see Section 13.2.

Step 5: Select one or more activities
The activities that you choose must be linked to your current situation and goals, and you need to determine the right tactics to adopt when selecting and deploying your activities. To this end, there are questions you need to consider, namely: what topics are you focussing on; what is your messaging when addressing these topics; and what are you targeting (i.e., people, processes, or technologies)? You also need to select the medians/activities you are going to use, for example: changes to policies/processes; software changes; awareness raising programmes (posters, email campaigns, etc.); training sessions; scenarios and wargames; using incentives, etc. When selecting activities, you must consider your resource constraints – i.e., can you purchase required materials/resources (off-the-shelf or bespoke), can you use internal staff to develop what is needed, or are you restricted to employing existing materials within the organisation?

Remember, always select activities that suit your organisational context and address the gaps you want to close (for a more detailed list of activities, see section 13.1.1).

Step 6: Run your selected activity
Run an activity individually if you want to be able to determine the specific impact of that activity. Run activities together as a joint-set is you want to determine their combined impact of those activities. You will need to monitor these activities closely while they are being run to ensure they are being conducted correctly – you should select the best method for achieving this based on the context of both the activity being run and your organisation's resources.

Step 7: Rerun current situation **metric and analyse the results**
After the activity (or joint-set of activities) is completed you need to rerun your CSC measurement and compare to the current situation and goals (Step 4) and analyse the results to identify impact (i.e., levels of success and any failures). You can also use these results to identify whether any positive/negative effects were universal across your entire target audience, or whether they varied by different sub-sets of your audience: e.g. specific age groups, business units, countries, roles, etc. These results then feed into Step 8.

Please note here that modifying both employee behaviour and the collective CSC within an organisation is a continuous process. This needs to be borne in mind when selecting when to remeasure the current situation, and how often to do this remeasuring – i.e., you may choose to undertake multiple re-measurements at

different time periods (e.g., 1 month, 3 months, 12 months, etc.) to understand how successful and resilient any behaviour modifications have been.

Step 8: Review and consider your results before deciding on next action

This step is your chance to review your strategy, based on your findings and experiences, and determine how the CSC proceeds going forward. If your CSC activities did not achieve your set goals, return to Step 5 and refine your activities or select a different [set of] activities and run again. If your CSC activities achieved your goals, or you wish to focus on a different aspect of CSC in your organisation, return to Step 4 and proceed. If you decide to change either your target audience or modify your goals, return to Step 3 and proceed. If, on the basis of your ability/inability to influence your organisation's CSC, you need to reassess your business processes and/or security measures, return to Step 2 and proceed.

5. Organisational requirements for a successful CSC

Developing a strong CSC is not a one-off activity, but is rather an ongoing process that needs to be continuously nurtured if it is to become embedded within the wider organisation's culture. It requires buy-in at the highest organisational level, with the engagement of the CEO and other senior figures with security responsibility being imperative. In this regard, senior employees need to act as champions for CSC, leading by example, and this should be backed-up by the allocation of resources (human and financial) to match the task at hand.

While senior buy-in is essential, the initiative to develop a CSC can come from anywhere within an organisation. Different initiation approaches include the following:

- **Top-down approach:** initiated by the Board, CEO and/or the most senior C-suite individual with responsibility for cyber security.
- **Mid-level approach:** initiated by mid-management with responsibility for cyber security or corporate culture (e.g. CSO).
- **Bottom-up approach:** initiated by an individual within a business unit who identifies a need.

However, regardless of who *initiates* a CSC programme within an organisation, the *on-going success* of these programmes is dependent on a number of common requirements. Firstly, while CSC programmes developed and run by a single person may have success in very specific areas, this approach rarely succeeds across the wider organisation. You need to assemble the right multi-department team with appropriate responsibilities to develop and deliver the programmes if they are to be successful across the entire organisation. Secondly, while the CEO/Board does not need to initiate a CSC programme, without their active, vocal support the programme is most likely going to fail.

In Section 12.1 below we discuss how to create a receptive environment to maximise the likelihood a CSC will develop within an organisation, while in Section 12.2 we provide guidance and details on the composition of a successful CSC implementation team.

5.1 Creating a receptive environment

An effective CSC should be encouraged and nurtured within the wider organisational culture in collaboration with the employees, rather than imposed, if the value of cybersecurity is to be accepted by all members. Changes to the working environment in the organisation require clear responsibilities and the involvement of everyone within the organisation, including senior management, fostering ownership of the program and the motivation to adhere to it. Commitment to cybersecurity should be signalled through sufficient budget allocation and motivation for greater security than simply compliance.

CSC can only be effective if employees have the tools, knowledge, skills and understanding of their role within it. There also needs to be acceptance of "this is how we do things" which will require a mix of approaches, all of which need to be people centric. While the CSC message needs to come from the top, it is important that employees have the ability to feedback on how CS can fit in with their current working processes. If CSC hinders or delays work progress, the more likely it is to be disregarded. Employees should be able to communicate any issues up the chain so that amendments can be made.

Engagement and participation is the optimum way to employees adopting a more CS oriented behaviour. Learning should be encouraged within a safe environment to prevent misunderstandings and defensive attitudes. Coercion should be avoided and dialogue should be encouraged – employees should be able to

ask questions and receive assistance as they get to grips with new procedures. Rewards should be used to reinforce and motivate secure behaviour and in parallel monitoring and sanctions can also act as compliance motivators. For a lasting culture change a combination of reward, clear responsibilities, and cybersecurity rules that are both aligned to business processes and do not conflict with other non-cybersecurity rules/processes, is more likely to be successful.

Increasingly, work extends outside of the workplace as employees travel and work from home. A strong CSC should do the same and CS should be presented as a "way of life" as the optimum way to strengthen protection against cyber-attacks. Culture also implies that the focus is not solely on technology and the ways in which people link with technology, but also on how they relate to each other and work together and the context within which this happens. Running awareness programmes or events that also tackle CS in the home through e.g., involving family members can be a good way to form a good CSC that extends across the work/home divide.

5.2 Assembling a CSC team

The first pre-treatment step in the process to set up a CSC within an organisation is to assemble a CSC team. The combination of members is important as you want to ensure:

- The legitimacy of your approach
- The longevity of your programme
- That you reach all levels of the organisation
- That your technological infrastructure is up to date and reflects the business needs of the employees
- That you know what your assets are and how to protect them
- That you engage the employees and provide them with relevant and suitable training materials
- That your approach is compliant and legal

While the contextual reality of each organisation differs (by size, organisational structure, responsibilities attached to roles, geographical distribution, existing culture, business sector, etc.) successful CSC development teams are typically comprised of a core set of individuals potentially accompanied by others drawn from across the organisation. Figure 8 displays the core and additional individuals. Please note that this structure will need to be tailored to reflect the specific distribution of roles/responsibilities within each organisation it is applied.

5.2.1 Roles and responsibilities

Senior Management - Member of the board or a high-level person for championing and signalling support for CS within the organisation and ensuring adequate resources (human and financial) to set up and maintain a strong CSC. Strategy formation and ensuring that CSC strategy and policies are embedded in the overall organisation strategy. As security and risk management are the responsibility of the senior management, their presence in the group should ensure that CS strategies and policies are embedded in broader security and risk management strategy. Senior management members can also assist with prioritisation to align with broader organisational interests. Senior management members will also communicate CS work to the board to ensure that the CSC at the upper levels is transformed to raising security risk awareness and preparing for swift reactions to breeches and incidents.

IT Department – to contribute their expertise in CS and ensure up-to-date technical measures, which are effective, simple, useful in supporting secure behaviour without being burdensome. CS expertise should be a core competency in the IT department and should be used as input for risk management, offering insights to senior management and supporting decision making.

Security/Information Security (CSO, CISO) – expertise in information security, good security governance, people and progress management. If the organisation has a CISO, she/he has a crucial role in the working group, to align IT and security goals, participating in the drafting of the CS strategy and policy and representing security at the executive level. To management and the board the CISO should offer information on the security developments, risks and possible courses of action in line with risk management principles. To employees the CISO provides clear, understandable and open communication, demonstrating that security is now part of "the way we do things".

Human Resources – Provides connection from management to the employees and oversee all staff-facing practices such as awareness raising, training and communication. HR also brings to the table knowledge insight into the behaviour of staff, their different roles and knows how to embed new practices within already established processes. HR can ensure that everyone goes through the same training and can oversee any evaluations, incentive schemes or disciplinary sanctions.

Legal – to ensure that all new practices contribute to the full compliance of the company with national and international legislation, including data protection. The legal department will also assist with defining what can be asked of employees within the remits of their contracts, and how to amend contracts if needed. If any of the CS practices involve monitoring employee behaviour, the legal department can establish that any monitoring falls within the boundaries of the law.

Marketing/Communication – As CSC is about changing mindsets, perceptions and conveying knowledge to people, the marketing/communications department will support the change by designing and promoting CS awareness and education programmes through developing impactful communication, and ensuring effective use of messages and channels for communication. A strong CSC can also be a strong marketing opportunity for an organisation, instilling trust in customers and business partners as CS concerns rise internationally. The marketing department can also establish strong CSC as a part of the organisational image, which also will strengthen it internally.

6. Elements and resources for successful CSC programmes

This section covers the elements and activities that are needed to construct a successful CSC programme. We list key activities that different organisations currently employ and provide some information on their use. As with the other elements of constructing a CSC programme implementation, the final selection of methods for delivering your CSC interventions is to be decided by your CSC implementation team, based on their knowledge of what is most likely to be effective within your organisation. For example, if you find that emails are a good way to reach your employees, use these. Here, the knowledge of your organisation is paramount to selecting the right activities for your CSC programme. In this Section we also advise on both the current situation calculation (proposing three ways to determine current situation in Section 13.2.1) and the production of effective metrics for measuring the impact of your CS activities (Section 13.2.2.).

6.1 Basic elements for constructing CSC programmes

6.1.1 CSC implementation activities

Organisations use a variety of methods to deliver CS messages and training to employees. Online methods, as well as offline and hybrid methods are useable for raising CS awareness amongst employees when creating a strong CSC. The method for delivery of CS messages should be chosen specifically for each organisation that fit with the current culture and methods of communicating. If it is a smaller company that is not highly technical in focus, a face to face approach might be more suitable for employees, while larger companies with technically adept staff may prefer online training and awareness programmes. You will also need to consider your resources available, the size of organisation, and staff working patterns when selecting your CSC implementation activities. If possible, different methods should be chosen to reach as broad an audience as possible and to allow for different styles of learning.

ONLINE	HYBRID	OFFLINE
Emails are an easy way of reaching everyone within an organisation. They can be used to deliver direct CS messages from the top (agenda setting, warnings of new threats etc), or used by HR to deliver new training materials such as videos, games, tip sheets, stories and FAQs. Emails are also the delivery tool for simulating phishing attacks, which will raise awareness of employees. It is helpful that all materials is also available to employees (e.g., on a company intranet) so that they can re-visit. Emails can be easily overlooked and are not effective as an only method to raise CS awareness.	**Run Scenarios, Rehearsals, Sandboxes, and War-gaming exercises**. Run scenarios/exercises with employees from one or more departments to: increase preparedness for cyber events; identify previously unrealised gaps-in/clashes-between processes; identify risks; increase appreciation of different unit's needs; create behaviours/responses that are produced [and owned] by the staff within the business units, rather than imposed by the security team.	**1-2-1 or group training sessions** – as with workshops, training sessions are a good way to provide an interactive learning environment, where employees can learn, test their skills, make mistakes and ask questions in a safe environment. While group training sessions can deliver the training for all employees, 1-2-1 sessions can deliver a targeted message for specific individuals that may have specific responsibilities with regard to CS.
Videos can be used for training and awareness raising purposes. They can also feature stories of good practice to demonstrate the value of a correct response to a cyber-threat. Videos can also feature talks by internal or external	**Stories** of employee good practice are an effective way to deliver relevant advice and learning material that employees can identify with. The stories can feature a response to a current threat, what measures the employee took and what the result was. Stories can be printed on	**Flyers**, like posters, can be effective at delivering short and easily-digested CS information and advice. They can also feature tips, FAQs, short stories and contact details for CS team. Flyers are a good way to reach both staff and others who visit your premises (e.g., clients and

experts or employees with CS responsibilities.	flyers or posters, told in a video or during online training.	business partners) and help broaden the audience of your CS message.
Games are increasingly used for training and education and CS is no different. Games and role playing facilitate engagement, participation and openness.	**Offer incentives** to promote 'good' behaviour and discourage 'bad' behaviour. These do not have to be large rewards (e.g., company merchandise, gift certificates, etc.). These can be linked to individual's behaviour or the behaviour of entire business units. Competitions can be run across the business with rewards to the 'best performing' team/unit.	**Workshops** allow for an interactive environment for employees to attend, receive training/information and they are also able to ask questions. Play around with different formats and focus – invite internal and external speakers. Ensure a supportive and positive environment so employees feel safe to ask questions and make mistakes.
Webinars featuring internal or external experts are an interactive a cost-effective way to deliver CS messages to employees. The webinars can also be saved and presented in an accessible place (e.g., the company intranet) for those employees who could not attend, or to re-visit aspects of the talk.	**Tip Sheets** are short lists providing easy access to key information about CS. They are aimed at giving advice on response to cyber threats in a clear and concise manner. These can be printed in flyer form, as posters or placed online on the company intranet.	**Events** focusing on general CS, a specific threat, tools against cybercrime allow for a more informal approach where people can attend talks, take home printed materials or CS merchandise. These could be extended to the families of employees, business partners and clients.
Online training courses are a good way to deliver CS training. Courses can be designed as "blanket" courses for all employees and/or specific target groups depending on organisation structure and focus.	**FAQs** like tip sheets are an effective way to organise information into easily navigated text. The FAQs can be printed as flyers or posters, or posted online for employees together with a search function.	**External expert lectures** are a good opportunity to get a broad and up-to-date understanding of CS issues and trends.
Organisation Intranet is a good place to communicate with employees about CS and allow access to CS materials (e.g., videos, FAQs	**Conduct 'mock attacks'**. These can include *online* attacks in the form of fake phishing emails sent to staff, through to *offline* attacks whereby physical access controls (i.e., entry to building procedures, visibly wearing the correct pass, etc.) are tested through the use of fake staff, or fake CEO fraud phone-calls are undertaken to test adherence to correct processes and procedures.	**Posters** can be used for a variety of purposes to highlight CS within an organisation. Posters can feature advice, tips on good resources, overview of threats, presenting new threats, provide advice and contact details etc.
Social media can be useful to communicate good CS habits, alert about specific threats, refer to good practices and useful resources. For this to work well, the organisation must have a strong social media practices and employees must follow its accounts.		

Figure 9: Selection of CSC activities for utilising to deliver CSC programmes

6.2 Measuring CSC programmes

You cannot quantify the impact of your future CSC programmes if you do not first establish an current situation that represents the current CSC level of your target. This holds true whether you are focussing on the entire organisation or specific business units/demographics within your organisation.

The broad nature of CSC, reflected in the definition provided in Section 1.1, means it is impossible to form a CSC as-is based on the measurement of a single action. Therefore, to create a quantifiable current situation, you need to divide CSC into dimensions/metrics that can be quantified and select appropriate data collection methods that actually measure the selected metrics. The importance of this last point should not be underestimated as care needs to be taken to ensure the selected metrics actually measure aspects of an organisation's CSC. Approaches for developing a CSC current situation and guidance on selecting appropriate metrics are presented below.

6.2.1 Different approaches for developing your current situation

There are three different approaches that can be employed by an organisation to produce a pre-treatment CSC current situation before they implement their selected programmes: one is to measure CSC separately from the treatments you are employing; the second is to use the selected metrics of the treatments as your current situation; while the third is to conduct both approaches one and two together. All three approaches are employed within organisations that have actively developed CSC programmes. We have outlined these below, along the inherent benefits and limitations of each approach. Before developing and deploying CSC programmes/treatments the CSC implementation team will need to decide which current situation approach to adopt based on their specific business context.

6.2.1.1 Approach 1: Determine a CSC current situation independently from your CSC interventions

Using this approach, calculating an current situation measurement or CSC 'score' for your organisation is achieved by conceptualising CSC as one or more dimensions to be measured via a data collection process. This CSC score is determined separately to your CSC interventions, hence is not a step included in the step-by-step implementation guide for CSC programmes in Section 2 (it would occur early in the pre-treatment phase). This approach employs the following process:

- Step 1: Collect data from/on your staff relating to aspects of behaviour, attitudes, awareness, etc., and calculate an current situation CSC.
- Step 2: Develop and implement your CSC interventions, employing the eight-step Implementation Framework detailed in Section 11.
- Step 3: Re-measure your CSC current situation at future intervals to determine changes in your organisational CSC levels.

Determining the CSC current situation requires either developing an in house methodology for conceptualising and calculating CSC or using external consultants and/or off-the-shelf products to achieve this for you. One off-the-shelf example is the Security CLTRe Toolkit[8] that breaks CSC into seven dimensions, measured by a staff questionnaire. These dimensions constitute metrics, with the analysis of the collected data providing your organisation's security culture score, both as an overall total and values for each dimension that can be mapped on a spider graph. The seven-metrics employed to measure CSC within the Security CLTRe Toolkit are presented in Figure 10.[9]

SEVEN CORE DIMENSIONS OF SECURITY CULTURE – THE SECURITY CLTRE FRAMEWORK

[8] https://get.clt.re/

[9] K. Roer and G. Petrič, Indepth insights into the human factor: The 2017 Security Culture Report, 2017.

Behaviours: Actual or intended activities and risk-taking actions of employees that have direct or indirect impact on security culture
Attitudes: Employees' feelings and emotions about the various activities that pertain to organizational security
Cognitions: Employees awareness, verifiable knowledge and beliefs regarding practices, activities and self-efficacy that are related to organizational security
Compliance: Adherence to organizational security policies, awareness of the existence of such policies and the ability to recall the substance of such policies
Communication: Ways employees communicate with each other, sense of belonging, support for security issues and incident reporting
Norms: Perceptions of what sort of security-related organizational conduct and practices are deemed normal by employees and their peers and what practices are informally perceived as deviant
Responsibilities: Awareness of the importance of every employee as a critical factor in sustaining or endangering the security of the organisation

Figure 10: CTRLe's seven dimensions for measuring CSC

Benefits: This approach provides an overall CSC picture/value for your organisation and/or business units enabling plotting of shifts in CSC over time. Additionally, multiple organisations and/or business units employing the same standardised CSC measuring instrument enables comparisons both between and within organisations, and the ranking of businesses/units – hence the CSC implementation team will be able to identify stronger and weaker areas within their business for the targeting of resources and programmes.

Drawbacks: This approach does not negate the need to develop additional metrics for individual CSC treatments – i.e., you still need to undertake pre- and post-treatment measurements with appropriately selected metrics for each CSC programme you implement, otherwise you cannot determine the effect of individual programmes. In addition, measurement tools based solely on self-completion questionnaires are affected by numerous biases (e.g., selective-reporting bias, providing desirable responses over reality, question patterns, etc.); while questionnaire designers/administers can employ techniques to minimise these effects, they cannot be completed mitigated. Finally, positive or negative correlations between overall CSC scores and the effects of CSC treatments does not imply causality.

6.2.1.2 Approach 2: Determine a CSC current situation by utilising your CSC intervention metrics

Using this approach, you develop your CSC current situation as part of the step-by-step CSC implementation guide by taking the results of the pre-treatment metrics and using these as your CSC current situation. This approach uses the physical manifestation of cyber-security relevant activities of staff as the CSC current situation of that organisation. This entails the following steps:

- Step 1: Create a list of metrics relevant to the cyber security activities of your organisation
- Step 2: Calculate pre-treatment values of these metrics through whatever data collection methods are most appropriate. These values constitute your current situation CSC
- Step 3: Develop and implement your CSC interventions, employing the eight-step Implementation Framework detailed in Section 11.
- Step 4: Re-measure these metrics by calculating their post-treatment values to determine any changes in your organisational CSC levels.

Example of applying Approach 2:

To produce their CSC baseline, the CSC implementation team at Acme Inc. begin by brainstorming a list of relevant metrics. A few examples from their wider list include the following:

- Desks clear of confidential documents at end of day
- Employee's [virtual] desktops logged-off when not at desk
- Not clicking on links from untrusted external sources
- Following reporting procedure for suspicious cyber activities

Having created their list of metrics, the CSC implementation team identify appropriate measurement methods:

- Desks clear of confidential documents at end of day: physical inspection by security staff or team leader
- Employee's [virtual] desktops logged-off when not at desk: log files
- Not clicking on links from untrusted external sources: employ fake phishing emails
- Following reporting procedure for suspicious cyber activities: employ an attack drill or conduct online knowledge test of reporting procedure

Before developing and implementing any CSC programmes targeting these metrics the CSC implementation team conduct pre-treatment measurements of these metrics – the results of which constitute the Acme Inc's CSC baseline.

Benefits: By selecting metrics based on specific behaviours, and then conducting pre- and post-treatment measurements, it is easier for the CSC implementation team to demonstrate the causal effect of their CSC treatment programmes. As a consequence, this enables the modification of future programmes based on the results, and demonstrated impacts can be leveraged for greater resource allocation. The list of metrics comprising the CSC current situation can be tailored to reflect the specific context and make-up of an organisation. Additionally, by employing the same measuring methods across an organisation, the results of different business units and/or sub-sets of employees can be compared by the CSC implementation team to identify stronger and weaker groups for the tailoring of future treatments.

Drawbacks: This approach reduces CSC to the specific behaviours covered by the selected metrics, and given the wide scope of behaviours, norms, beliefs, attitudes, etc., that comprise CSC, this CSC current situation is likely to represent only a subset of the wider CSC within an organisation. The bespoke nature of this approach prevents standardised comparisons of current situation CSC *between* different organisations, making it harder to identify how one organisation compares to others in a similar space.

6.2.1.3 Approach 3: combine approaches 1 and 2

Given that (a) both of the two previous approaches possess unique benefits, and (b) many of the drawbacks of each approach are addressed by the other, the CSC implementation team may choose to employ both approaches 1 and 2. If this third, combined approach is adopted, the CSC team may select to measure the *overall CSC score* (as outlined in approach 1) on a periodic basis (e.g., annually, bi-annually, etc.) to provide a higher-level picture of your organisation's CSC, while measuring specific behaviours as part of your ongoing CSC activities (as outline in approach 2).

6.2.2 'Good' versus 'bad' metrics for measuring success

Metrics are necessary for both establishing CSC current situation and measuring the impact of CSC programmes. When selecting such metrics, organisations already recognise the need to utilise those that are relevant to both the context of their organisation and their organisation's security goals. However, aside from any contextual requirements, it is important for CSC implementation teams to appreciate that not all metrics that measure *cyber security* can be utilised to measure *cyber security culture*. In this respect, for the specific purpose of measuring CSC there are both 'good' and 'bad' CSC metrics:

- A ***good*** CSC metric is one tells the implementer something of value about the culture of cyber security within an organisation.
- A ***bad*** CSC metric is one that does not provide the implementer with valuable information about the organisation's cyber security culture regardless of whether it pertains to cyber security.

Good and Bad metrics in practice:

It is accepted good practice that organisations should have a cyber security policy, but such policies can only impart value if employees are familiar with its content. As a result, the ISO at Acme Inc. conducts an online training programme to familiarise employees with the policy. She wishes to measure the *awareness* impact of this programme which requires selecting a suitable metric.

- A poor metric here would be to measure the number of employees who undertook the training. While this is quantifiable it provides no information of value on the how aware employees are of the actual content of Acme's cyber security policy.
- A good metric would be to test employees' knowledge on the content of this policy by conducting pre- and post-testing either side of the online training programme, as the data collected pertains directly to the CSC of Acme Inc.

In addition to the requirement that selected metrics provide valuable information of an organisation's CSC, there is the practical requirement that the CSC implementation team must be able to collect data on their selected metrics if they are to conduct the necessary pre- and post-measuring. This practical requirement will be determined on an organisation-by-organisation basis, dependent on the capabilities of each organisation. To assist CSC implementation teams here there exists a range of methods and vectors that can be tasked for collecting measurement data. These include the following:

- Utilising existing software and hardware technology reporting: Reports from servers, IT security tools, and log files. e.g. number of attacks and number of breeches that are picked up from IT security and antivirus software.
- Sending out surveys with questions to employees regarding their cyber security awareness. These consist of either qualitative or quantitative questionnaires, or a mix of both
- Security reporting: e.g., number of lost/stolen devices
- Sending out phishing emails and malware campaigns to measure employee response, e.g., how many people "click the link".
- Monitoring employee IT activities in general, whilst recognising boundaries of privacy. Focus here might be more on a team or department level to avoid focusing surveillance on specific individuals.

6.2.3 Examples of 'good' metrics employed by organisations

Figure 11 below sets out a number of metrics drawn from existing resources/literature and currently being employed by different organisations within their CSC programmes that met the 'good criteria' identified in Section 13.2.2 above. Please note that this is not intended to be an exhaustive list, nor are we suggesting you must (or indeed should) use these specific metrics within your own CSC programmes. As with all the guidance presented in Section 13, you must contextualise the selection of metrics to your own organisation and CSC requirements: i.e., metrics related to bring-your-own-devices or maintaining a clean-desk only make sense if such devices are enabled and you maintain an office. Similarly, if your organisation lacks the ability to measure a specific behaviour linked to a metric (whether because of technical, staffing, legal or financial constraints) then that metric will necessarily need to be rejected.

POSSIBLE METRICS FOR ESTABLISHING THE CURRENT SITUATION AND MEASURING SUCCESS OF CSC ACTIVITIES
Number/percent of employees who fall victim to a fake phishing attack.
Number/percent of employees following reporting procedures after detecting a [fake] phishing attack.
a) Number/percent of employees who display understanding of security policies, processes and standards (potentially measured through testing) b) Number/percent of employees who display they are acting according to security policies, process and standards (CSC team may choose to select specific items from the policy and develop testing measures accordingly)
Number/percentage of devices that are updated and current according to policy
Number/percent of devices that are encrypted as per the organisation's policy (may choose to focus on specific devices used to physically transport data – i.e., memory sticks, hard drives, etc.)
Number/percent of employees who are securing their desk environment before leaving, thereby following the organisations policy
Number/percent of employees whose password structure meet the organisation's requirements
Number/percent of employees who can identify, stop and report a social engineering attack
Number/percent of employees posting sensitive organisational information on social networking sites
Number/percent of employees who are properly following data destruction processes
Number/percent of employees who follow physical security policy on restricting access to individuals who are not carrying and displaying a valid pass

Figure 11: Example metrics for use in Current situation setting and measuring the impact of CSC activities

7. Good practices from deployed CSC initiatives

Based on a combination of desktop analysis and interviews with CSC professionals within organisations across Europe, a number of good practices were identified. These have been presented below, divided in two ways based on the specific target audiences.

7.1 Good practices targeting different seniority levels within an organisation

Figure 12 presents identified good practices, arranged according to the seniority-level of employees within an organisation, covering the spectrum from board-level to non-management.

TARGET AUDIENCE	GOOD PRACTICES
Board Level	Set cyber security as a standing agenda item at board meetings – thereby signalling your support to CSC to the broader organisation.
	Require ultimate cybersecurity responsibility is assigned to a sufficiently senior C-suite manager that is either on the board or reports directly to the board.
	Require periodic information on both the state of cyber security culture within the organisation, and the measures and resources assigned to fostering the continued shaping and maintenance of this culture.
Senior Management	Be a part of the organisation CSC working group so that you can provide direction, signal support, assist with strategy and policy making and ensure adequate resources
	Deliver status reports up to the board and direct any messages downstream as well
	Be visible in your support for CS and champion the issue in your practices and speech. This entails also ensuring senior management: undertakes at least the same CS training as all staff; is a full target of CSC activities; and does not assign itself special dispensations not to follow and be bound by the same rules as other employees.
Middle Management	Communicate and champion CS to your employees. Assist with any queries.
	Ensure that employees are consulted and heard in their concerns, by transmitting their messages up the chain to the CSC group. This way, solutions can be made to complement their working practices.
	Monitor CS behaviour and oversee compliance.
	Be vocal and proactive in identifying where CS policies/practices and other business policies/practices clash in their day-to-day operation. Maintain this posture until the CS practice and/or the business practice is changed or removed – a conscious decision that needs to be based on the organisation's risk appetite.
Employees	Engage with the CS messages in your organisation. Attend training and awareness raising events and follow CS procedures.

	If you feel CS solutions or practices are hindering your work, don´t ignore them. Escalate your concerns to your line manager.
	Challenge those who are not following correct security procedures.

Figure 12: Good practices per seniority level

7.2 Good practices targeting different roles operational roles within an organisation

Figure 13 presents identified good practices, targeted at specific departments and roles within an organisation.

TARGET AUDIENCE	GOOD PRACTICES
Security	Provide the security focus and expertise to the CSC working group
	Ensure clear security communication to employees and make sure they understand why they should care about security and CS and exactly what is expected of them.
	Ensure that there is a clear CS point of contact within your organisation.
	Develop an understanding of the organisation, i.e., talk *with* (not *at*) the different business units to understand exactly what process they need to undertake to do their job so as to collectively agree on: (i) which security processes *complement* these business processes; (ii) where *compromises* can be made to ensure an acceptable working harmony between the CS and business processes; and (iii) where *conflicts* exist that cannot be resolved – in this situation escalate this conflict to the appropriate [risk] committee so the business can decide whether to abandon the business practice or accept the risk are remove the CS measure.
IT Department	Contribute your IT and CS expertise to the CSC working group.
	Build or implement supportive IT infrastructure and technology which assists employees in the protection against cybercrime.
	Ensure that technologies are implemented that can provide useful insights into CS behaviour and attacks, so that data can be easily gathered for analysis and integrated into the CSC programme.
CSC Implementation Team	Ensure that metrics and current situation setting are accurately set before any activity is commenced.
	Ensure clear communication within CSC team and between the team and rest of the organisation.
	Analyse the findings after each implementation cycle in order to amend your approach.

8. The case for implementing a cybersecurity culture

8.1 Economic costs of cyberattacks and breaches

The economic costs of breaches can encompass both direct costs (e.g. loss of intellectual property or data) and indirect costs (e.g. loss of reputation and/or market power). Losses can take multiple forms, including downtime of services, compromise of confidential information, fines for personal data breaches (see below) and decreased profits through reputational damage. In 2016, information and revenue losses, together with costs of business disruption, accounted for 95% of breach costs.[10]

Although exact figures are difficult to quantify, especially losses due to denial of services to clients, cyberattacks can result in great costs and losses. A 2014 McAfee and Intel Report estimates that global cybercrime caused between €325 and €500 billion in losses. While the costs of a data breach vary by country and industry, in 2017 the average cost of a data breach was €3.14 million, with every lost or stolen record with sensitive or confidential information costing €122. Costs fell compared to 2016, however, the average size of data breaches increased by 1.8% with an average of 24,089 records breached per country or region globally.[11]

Attacks numbers have risen significantly in recent years. Between 2015 and 2016, a fourfold increase in the volume of spam and malicious attachments was detected[12] with 229,000 attacks blocked daily in 2016.[13] No company is safe, regardless of size, with financial gain being by far the biggest motivator for cyberattacks in 2016[14]. Cyber threats are now a business enterprise, with notable developments in ransomware between 2015 and 2016 marked by an increase in diversity, number of detections, and a fourfold increase in the average ransom amount demanded. In addition, global risk exposure to cyberattacks has risen thanks to global value chains with companies are increasingly dependent on each other.[15]

On a positive note, an overall higher awareness of cybersecurity and investment in up-to-date technology and practices among all actors online can raise the immunity of everyone and slow the spread of cyber threats significantly. This suggests investments in CSC can lead to economies of scale among Internet users and could even be considered a part of a company's corporate social responsibility. Security is important for customers as well with the biggest financial consequence of cyberattacks for companies being lost business due to falling consumer trust, especially in regulated industries. A strong CSC can be leveraged to improve trust, not only within a company but also with customers and business partners.

Finally, investment in cybersecurity technologies and practices can support business innovation and significantly reduce both costs and losses. Business innovation, through expansion, specialisation or new technology adoption is necessary to maintain competitiveness, and a robust CSC embracing an awareness program is the most cost-effective security control for managing the security risks of new technologies.[16]

---

[10] 2016 – Ponemon Institute – Cost of Cyber Crime Study and the Risk of Business Innovation, p. 12.
[11] 2017 – Ponemon Institute – Cost of Data Breach Study
[12] 2017 – IBM – X-Force Threat Intelligence Index
[13] 2017 – Symantec – Internet Security Threat Report
[14] 2016 – Verizon – Data Breach Investigations Report.
[15] 2011 – McKinsey – Meeting the Cybersecurity Challenge, p. 3.
[16] 2007 – Yanus, Shin – Critical Success Factors for Managing an Information Security Awareness Program; Albrechtsen, E. and Hovden, J., 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An Intervention Study, Computer and Security, 29 (4), 432–445.

8.2 Policy guidance and impact

Organisations do not have to act alone when fostering their CSC. The public sector can assist through educational campaigns, standardisation and certification initiatives that can influence the skills, knowledge and incentives of people and companies, facilitating the development of CSC.

Education is a field in which public policy may be especially impactful. Recent studies have pointed to a world-wide shortage of cybersecurity professionals, despite the high remuneration offered. This leads to insufficient cybersecurity resources resulting in increased stress and long hours for IT professionals and can precipitate human mistakes. Since the IT and security teams in an organisation make critical contributions to the content of the culture transformation, investments in their education lies at the basis of a good CSC.

Public education initiatives can champion cybersecurity as a core aspect of any IT education and can ensure that new technologies and practices form a part of that, and IT specialists need to adapt to the new environment of cloud computing, bring-your-own-device, incidence response and information risk management. An example of public support for cybersecurity education is the 2010 National Initiative for Cybersecurity Education (NICE)[17], led by the National Institute of Standards and Technology (NIST) in the US. The NICE programme focuses on awareness, formal education, workforce structure, training and professional development for all, and has prioritised: the acceleration of learning and skills development; diversification of the cybersecurity workforce; and the career development and workforce planning of cybersecurity professionals.

The perceptions and knowledge of the general population may also be impacted through educational policies and general value statements, with a clear political will towards cybersecurity capable of changing national attitudes. Prioritising CSC in national cybersecurity strategies, and offering unbinding guidelines, research and information to companies can further facilitate CSC., with such national campaigns proving especially beneficial for SMEs.[18]

Standards can also support the development of a CSC, as they can present useful frameworks for incorporating into their CSC while influencing company incentives to implement a CSC programme. Standards can cover both technical and operational aspects, and can guide security managers and IT staff regarding cybersecurity plans and strategies, as well as specific roles and responsibilities. Existing popular security management standards already cover broad areas, including: information security policy; communications and operations management; organisation of information security; asset management; incident management; business continuity; human resources security; and compliance.

International and national authorities can aid the development of CSC by adopting, promoting and supporting current industry-specific standards, based on sound and thorough research of best practices. While standards are general and universal, organisations are encouraged to adapt useful security practices and frameworks to their own risk profile and industries. A 2016 study among IT and security professionals in the US found that 84% of organisations had already adopted some security framework to for guidance, the most popular ones being the Payment Card Industry Data Security Council Standard (PCI), ISO/IEC 27001/27002, CIS Critical Security Controls and the NIST Framework for Improving Critical Infrastructure Cybersecurity. Moreover, 44% used more than one framework, as organisations take advantage of frameworks and tailor them to the needs of their organisations, business models and business partners.

[17] [17]https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan
[18]2007 – Dojkovski – Fostering Information Security Culture in SMEs

Finally, compliance with robust standards may be used to achieve certifications. Certificates can demonstrate security and trustworthiness to potential business partners and customers and can incentivise compliance with standards thereby fostering a CSC. National and international authorities can, thus, use standards to support the development of CSC within organisations.

8.3 Legal aspects: liabilities / or Regulatory and legal aspects

Regulatory aspects can impact how a company develops their CSC and in light of increasing cyberattacks and privacy concerns, the regulatory risk of changes to legislation must be prepared for as new administrative burdens are likely to arise. Regulation can impose additional costs for companies, and the subsequent design, execution, documentation and updating of security policies must correspond to the regulatory responsibilities of companies towards their clients, employees, business partners.[19]

Legislation can also obligate standardisation of security programmes by specific organisations. For example, the 2016 Directive on Security of Network and Information Systems (the NIS Directive) establishes security and notification requirements for operators/providers of digital and/or essential services and envisions penalties and enforcement procedures against companies, which have failed to fully abide by security requirements. As a result, measures to prevent and minimise the impact of any breach must be undertaken, and adopting a culture of risk management is listed among the responsibility of these operators.[20]

Legal responsibilities and liabilities can also influence organisations. Due to the size and cost of information security breaches, involvement in the cybersecurity of their organisation by officers and directors should be considered part of their fiduciary responsibilities. While reasonable care must be employed when taking decisions, the standard of what is reasonable is not static, reflecting the different risk profiles of organisation, as well as evolving state-of-the-art technologies and practices. Legislation, such as the Sarbanes-Oxley Act in the US creates legal obligations for senior management and the Board to continuously consider, ensure and report on information security.[21] This reinforces the importance of updating policies and maintaining senior management involvement.

Finally, companies could face fines for data breaches, which affect users' personal data. The General Data Protection Regulation (GDPR), which enters into force in 2018, imposes stricter security and standard obligations for both companies and their sub-contractors.[22] Furthermore, it mandates quick notifications of data breaches by companies to authorities and users,[23] increasing the potential for reputational damage. Finally, hefty administrative fines of up to €20 million or 4% or annual global turnover (whichever is higher) can be imposed for breaches of data protection and security requirements.[24] Such fines represent compelling arguments for embedding cybersecurity protection through a CSC.

8.4 The importance of human factors in cybersecurity

Despite the majority of cyberattacks in 2016 being hacking and malware-related, three of the top five cyberattack threats were related to human factors, these being; social engineering through phishing emails, human errors, and deliberate misuse.[25] In 2015, 21.8% and in 2016, 15.8% of all data breaches were due to phishing, spoofing or social engineering, while in 2017, human errors accounted for between 19 to 36% of

[19] 2015 – Foley & Lardner LLP – Taking Control of Cybersecurity, p. 3.
[20] Preamble (44), Articles 16, 17 NIS Directive
[21] 2013 – Business Software Alliance – Information Security Governance
[22] Article 32 GDPR
[23] Articles 33, 34 GDPR
[24] Article 83, GDPR
[25] 2016 – Verizon – Data Breach Investigations Report.

all data breaches, depending on country or region.[26] In addition to cyber-based threats there is the additional challenge of ensuring physical security when discussing human operators, especially when faced with insider-threats, as cybersecurity encompasses intrinsic human/physical elements. Policies covering maintaining a clean-desk free from classified document, locking screens and systems when away from a computer, challenging staff not displaying ID badges on business floors, and enforcing building access controls, are all physical protection measures that must be incorporated into an organisations CSC.

The human contribution to cyber risk is clear. However, imparting knowledge, enhancing awareness and influencing employee behaviour to mitigate these risks are difficult tasks and ignoring human factors in the development and deployment of cybersecurity policies and processes predestines these activities to failure. Staff will actively seek to circumvent security policies that: prevent them from completing their designated business functions; impose what they consider to be an unjustified burden; and/or represent a lack of understanding as to what should be prioritised. This is usually not out of maliciousness or ambivalence, but out of a desire to 'successfully do their job'. For example, strict corporate policies on the use of private devices for work may be viewed as unnecessarily burdensome among employees. Imposing multiple, complex passwords to be changed regularly without allowing password keychains forces staff to write their passwords down to memorise them, possibly using electronic means. Computers in hospital emergency departments are left 'logged-in' by staff (against security policies) who prioritise the immediate treatment of patients to save their lives over the protecting of patient data.[27]

Additionally, humans possess a finite capacity for complying with security requests within the workplace. Beyond a certain threshold, any attempts to impose additional security procedures and requirements will be met by resistance and attempts to circumvent. It has been noted that in many workplaces, this threshold for compliance has long been exceeded by most users.[28]

The development of a CSC is important to manage the risk of the human factor, while enabling the adoption and use of new technologies by companies. Effectiveness, flexibility and adaptability should be pursued, supported by a strong culture of cybersecurity. Innovations, such as adopting a bring-your-own-device policy or acquiring a new business partner can make organisations exposed, but they are necessary to maintain competitiveness and growth. A good CSC will instil a security mindset in people in all facets of their work and may even spill over to their private life.

[26] 2017 – Ponemon Institute – Cost of Data Breach Study
[27] ENISA, Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures, 2016.
[28] Herley, C. More is Not the Answer.

9. Organisational factors impacting cybersecurity cultures

Organisations can take steps to shape both their CSC and wider organisational culture can greatly influence CSC. Here, collaborations within the organisation are essential as open communication will facilitate the development of a CSC. While everyone within a company should be involved, contributing their fields of expertise, identifying where cybersecurity risks and other business functions intersect, and potentially conflict and brainstorming solutions, certain executive positions and departments have a key role to play in the development of the CSC. These factors are examined below.

9.1 Organisational culture

Organisational culture is a complex system of shared beliefs and values among employees, which guides their behaviour, or to put simply, it is the way things are done. The employees' information security views, attitudes and behaviours will in turn be affected by changes in the organisation's information security culture.' Organisational culture can reinforce commitment to the organisation and enhance stability by offering guidance and accepted standards for employee behaviour. Both acceptable and unacceptable behaviour should be defined in line with the organization's wishes and encouraged or denounced respectively. If sanctions are enforced, consistency in their application is needed to ensure compliance and influence changes in the mindsets of employees.[29]

Against this backdrop, an effective CSC should be fully embedded within the organisational culture if the value of cybersecurity is to be accepted by all members. Changes to the working environment need to be visibly endorsed by senior management, and operationalised through clear responsibilities and involvement by everyone within the organisation, fostering ownership of any program and motivation to adhere to it. Commitment to cybersecurity should also be signalled through sufficient budget allocation and a motivation for achieving greater security, rather than simply compliance with ticking boxes. Indeed, a commitment to quality and cybersecurity suggests a wider organisational culture of excellence in business.[30]

9.2 The organisation's wider cybersecurity strategy

A pre-requisite for a CSC is the development and communication of policies and procedures, which lay down clear responsibilities and serve to guide security behaviour and attitudes. Based on an initial assessment of the current state of security culture, management should draft a cybersecurity strategy incorporating a policy to guide the cultural change and define security goals and the organisation's vision.' In so doing, specific goals and end-user usability should be fundamental considerations, as permanent behavioural changes are possible only when they equate to success and satisfaction among employees.

To facilitate employee ownership, acceptance and support, everyone in a company should be encouraged to participate when developing and embedding an information security policy. This ensures that security measures are adapted to the functional and hierarchical differences within the company and that they are avoid becoming too burdensome or complicated.'

A successful strategy should: (1) reinforce strong governance attitudes and actions; (2) be designed similarly to other business functions to ease acceptance; (3) be built around an adaptable framework to facilitate long

[29] Alnatheer, Understanding and Measuring Information Security Culture, 2012.
[30] RAND, Cybersecurity economic issues, 2008.

use; and (4) its effectiveness should be measurable to demonstrate success. The use of metrics here can aid management in reviewing and updating policy through regular monitoring and assessment of impact.

9.3 Cross-organisational commitment – the roles to be played by different groups

9.3.1 The role of senior management

Cyber security has become the responsibility of senior management, driven by the financial and reputational risks of breaches, regulatory requirements and pressures exerted by shareholders. Beginning, transmitting and embedding cultural change requires leadership and buy-in by senior management, and to ensure this change is lasting, it should clearly signal its commitment and involvement in CSC by allocating sufficient resources for comprehensive programmes while delegating clear responsibilities and authority.[31, 32]

Senior management and the Board should treat cybersecurity as a risk to be accounted for and make strategic decisions on the security requirements of their organisation by examining the implementation of possible policies and technical measures. In this regard security should be viewed not simply as a cost, but a risk reducer. Furthermore, clear priorities must be established and communicated to the CISO, enabling him/her to carry out their duties in alignment with the company risk appetite, interests and requirements.

Finally, to change culture, senior management must use a range of instruments, including value statements, internal communication, education, and must lead by examples through their behaviours supporting their visionary statements. Robust CSC within management is evidenced by raising security risk awareness, conducting security breach reaction and continuity drills, and improving communications with the CISO.

9.3.2 The role of CISOs

The CISO has a crucial role in developing a CSC. She/he must understand the needs and operations of their business, while using their technical and communication skills to align IT and security goals with business ones. CISOs such participate in drafting the cybersecurity strategy and represent security at the executive level, while maintaining good communication channels with both senior management and employees to effectively share their vision.[33]

To management and the board, the CISO should make clear the value of cybersecurity, while offering information on security developments, risks and options in line with risk management. To employees, the CISO must engage in clear and understandable communication, involvement and support activities, demonstrating that security is part of "business as usual" rather than an impediment to business activities. CISOs are responsible for good security governance, people and process management. Participation in decision-making and the shared understanding between the stakeholders is important and may be facilitated through committees, liaison roles, open communication, and social participation throughout the entire transformation process.[34]

9.3.3 The role of middle management

As the intermediary between employees and senior management, middle management has a key role to play in setting the tone of cybersecurity in an organisation. They need to be convinced of its benefits and should be effectively involved in the implementation of cybersecurity throughout the organisation. To avoid

[31] 2013 – Business Software Alliance – Information Security Governance

[32] Alnatheer – Understanding and Measuring Information Security Culture, 2012.

[33] D. Ashenden, "Information Security management: A human challenge?" Inf. Secur. Tech. Rep., vol. 13, no. 4, pp. 195–201, Nov. 2008.

[34] 2005 – Koh – Security Governance – Impact on Security Culture. (maybe get other footnotes too, p. 3-4)

cybersecurity being treated as an impediment and burden by the teams they lead middle management should insist on and encourage secure behaviour by offering feedback and motivation for employees, both regarding their business and IT performance.

9.3.4 The role of the IT

The role of the IT team in CSC is multifaceted. The team should ensure that up-to-date technical measures are adopted, which are effective, simple, useful and support secure behaviour by not being overly burdensome. To effectively achieve these aims by tailoring solutions, those maintaining the technical infrastructure must understand the business structure of their organisation and its activities, while the open communication of IT objectives, milestones and processes can further guide the CSC programme.[35]

Expertise in cybersecurity must be a core competency in the IT department, implemented either through a specialised team or by collaborating with external service providers. This cybersecurity expertise should inform risk management, supporting the decision-making of CISO's and offering insights to senior management. It can also be leveraged to drive the development of security education and the adoption of preventative technologies throughout an organisation.

The collection of data regarding cyber risks and attacks against the organisation's networks should be ensured. Data regarding the cybersecurity performance of the organisation can be used to re-evaluate and update the company's incidence response programmes, bring an in-depth understanding of its risk profile, and measure the impact of any implemented CSC programme.

9.3.5 The role of legal/compliance

The legal/compliance department has a role to play by offering expert legal advice to ensure any CSC and cybersecurity practices embedded in the organisation comply with national and international legislation, including data protection norms. The department should also provide support when implementing technical measures geared towards monitoring employee behaviour, to establish that what is being monitored and how the information is utilised is fully compliant with national and trans-national legal requirements.

9.3.6 The role of human resources

Human resources (HR) have an important role as a connector between management and employees. Thanks to their position within an organisational, HR can offer insights into the behaviour and psyche of employees, which in turn can be used to counter potential insider threats or design and deliver effective security education programmes. The department can also ensure that everyone in the organisation undergoes the necessary security training by enforcing compliance while conducting security practice evaluations of employees and, where necessary, enacting disciplinary sanctions.[36, 37]

9.3.7 The role of marketing/internal-communications

CSC is about changing mindsets, perceptions and conveying knowledge to people, with security presented to employees as "business as usual". The marketing department can assist CSC development by designing and promoting security awareness and education programmes, and producing messaging that maximises

[35] 2017 – RSA – Translating Security Leadership into Board Value
[36] 2000 – Nosworthy – Implementing Information Security in the 21st century
[37] 2014 – PCI Security Standards Council – Best Practices for Implementing a Security Awareness Programme

impact and emphasise the benefits of CSC. They can also maximise cost-effectiveness by leveraging personalised approaches and multiple channels.[38, 39]

Cybersecurity can also be employed as a powerful marketing tool for attracting customers and business partners, especially as privacy and cybersecurity concerns rise globally. Corporate social media activities, managed by the marketing department, can present cybersecurity as a key aspect of a corporation's image, shining a light on and reinforcing the internal CSC of that corporation.

9.4 Adopted business and employment models

Today's flexible business models can impact the CSC of an organisation. New and temporary employees (such as consultants or contractual agents) that are less integrated into an organisation won't be as influenced by the organisational culture. To develop a CSC, special consideration must be afforded to communications and training for *all* categories of employees, and this training must be continually reviewed to encompass changes in technologies and working practices.

Business dependence on internet access continues to grow, while working environments increasingly allow "bring-your-own-device" policies that open new risk exposures. At the same time, the weakening of distinct boundaries of responsibility for companies integrated into the wider networks of others, and the increase in global value chains and business partnerships all lead to growing risk exposures. A robust CSC, in combination with security contractual clauses[40] and risk assessments of new business partners[41] can contribute to achieving enhanced information security.

[38] 2013 – Ashenden – CISOs and Organisational Culture – Their Own worst enemy
[39] 2014 – PCI Security Standards Council – Best Practices of Implementing a Security Awareness Programme
[40] 2012 – Deloitte, Risk Intelligent Governance in the age of cyber threats, p. 10; 2000 – Nosworthy – Implementing Information Security in the 21st century
[41] 2015 – Foley & Lardner LLP – Taking Control of Cybersecurity

10. Non-organisational factors impacting cybersecurity cultures

CSC is the way employees act with regard to cybersecurity, to protect the organisation's information assets or to achieve the desired level of cybersecurity, as well as their underlying knowledge, beliefs, perceptions, attitudes, assumptions, norms and values. Developing an effective CSC requires recognising and utilising factors outside of organisational science and management. Understanding the impact of human psychology, sociological factors, and cultural impacts is essential for the development of a successful CSC. After all, employees are first and foremost human beings navigating both their workplace (organisational) environment, as well as wider social pressures.

This concept of culture can encompass repeated behaviours,[42] group norms,[43] embedded skills,[44] shared meanings,[45] and formal rituals and celebrations.[46] Through the invisible structures they offer, these ideas, behaviours and social customs facilitate and guide the beliefs and interactions of organisation members. It is the social aspect of culture that leads to the natural development of shared sets of beliefs among people,[47] and as a security is also a mental attitude, it must be embedded in the organisation's value system through culture transformation before an organisation can speak of its cybersecurity culture. What is essential for promoting, developing and embedding CSC, is that existing organisational cultures can be transformed.

To assist in the understanding of this process, culture can be divided into three levels that interact together: (1) promoted values, (2) visible behaviours, and (3) the underlying assumptions we hold.[48] An organisation's culture transformation should begin with a change in values, leading to the adoption of new behaviour. If that behaviour is successful in solving a problem, it will likely be adopted permanently and the value will transition into an underlying assumption.

10.1 Human factors that impact cybersecurity cultures

Security technologies can only be effective if employees have the necessary knowledge, skills, understanding and acceptance to use them.[49] Achieving this 'human security' may require a change in both the knowledge and behaviour of employees,[50] whereby education and training may be used to foster knowledge, while behaviour can be altered through cultural and organisational incentives and sanctions.[51]

10.1.1 Psychological factors

To convince people to change, three parallel processes must take place: (1) there must be dissatisfaction with the current situation; (2) this dissatisfaction must cause anxiety and/or guilt; and (3) employees must

[42] 2004 – Schein – Organizational Culture and Leadership, p. 12; Goffman, 1959, 1967; Jones, Moore, and Snyder, 1988; Trice and Beyer, 1993, 1985).
[43] Homans, 1950; Kilmann and Saxton, 1983.
[44] Argyris and Schön, 1978; Cook and Yanow, 1993; Henderson and Clark, 1990; Peters and Waterman, 1982.
[45] Geertz, 1973; Smircich, 1983; Weick, 1995.
[46] Deal and Kennedy, 1982, 1999; Trice and Beyer, 1993.
[47] 2005 – Van den Steen – On the Origin of Shared Beliefs (and Corporate Culture)
[48] 1985 – Schein – Coming to a New Awareness of Organizational Culture
[49] K. Roer, "How to build and maintain security culture," 2014. S. Furnell and K. L. Thomson, "From culture to disobedience: Recognising the varying user acceptance of IT security," Comput. Fraud Secur., vol. 2009, no. 2, pp. 5–10, Feb. 2009.
[50] 2005 – van Niekerk – Establishing an information security culture in organizations
[51] 2005 – van Niekerk – A Holistic Framework for Fostering IS sub-culture in organizations

be able to adopt new behaviour in a safe environment without compromising their identity or integrity.[52] To "unfreeze" the existing culture, its shortcomings must be identified and communicated, after which the new culture can be instilled by changing knowledge and behaviour. This must be conducted in a safe learning environment to prevent anxiety and defensive attitudes against the new culture; coercion should be avoided, as it would increase defensiveness and decrease acceptance of change.[53] Rather, people must be engaged in the culture so that they participate in to, contribute to it and feel responsible for it. This can be achieved through accountability, trust, communication and cooperation within the organisation.

Individual personality traits can also affect the security behaviour and attitudes of people, whereby conscientious and diligent staff tends to be more aware of and comply with security, as do longer-term staff.[54] Openness and experience can encourage security confidence, while neuroticism and emotional instability have the opposite effect.[55] However, given the right circumstances open individuals, neurotic and extrovert staff are more likely to violate cybersecurity policies.[56] Finally, an individual's level of risk perception and aversion can lead to differences in behaviour.[57] All this considerations must be taken into account when designing a security culture transformation.

Gender may also influence employee behaviour and attitudes, as men tend to be more confident in their security behaviour and privacy attitude online than women,[58] although women generally perceive vulnerability more and are more likely to behave securely. [59] Men seem to be influenced by attitude towards technology, while women by social roles, behavioural controls and norms.[60] To instil CSC, a gender balanced workplace and appropriate framing of the new culture are necessary.

10.1.2 Compliance and personality

As security programmes demand additional effort, employee behaviour may be influenced by the perceived costs and benefits of security compliance,[61] such that to persuade staff to act securely, risk perception is key.[62] For achieving lasting change, people should understand: (1) the threats they are faced with; (2) the security policy they must comply with; and (3) the responsibility they carry.[63]

---

[52] 2004 – Schein – Organizational Culture and Leadership, p. 320, 335.

[53] 2005 – van Niekerk – Establishing an information security culture in organizations, 2004 – Schein – Organizational Culture and Leadership, p. 329.

[54] 2017 CLTRe Report

[55] 2016 – Halevi et al – Cultural and Psychological Factors in Cybersecurity

[56] 2012 – McBride – The Role of Situational Factors and Personality

[57] O'Neill, B. (2004). Developing a Risk Communication Model to Encourage Community Safety from Natural Hazards, paper presented at the Fourth NSW Safe Communities Symposium, Sydney, NSW.

[58] 2016 – Halevi et al – Cultural and Psychological Factors in Cybersecurity; 2016 – Anwar et al – Gender Difference in employees and cybersecurity behavior.

[59] Hearth, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance inorganizations. European Journal of Information Systems,18(2), 106-125; Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. Computers & Security, 31(1), 83-95.

[60] Morris, M. G., Venkatesh, V., & Ackerman, P. L. (2005). Gender and age differences in employee decisions about new technology: An extension to the theory of planned behavior. IEEE Transactions on Engineering Management, 52(1), 69-84.

[61] 2008 – Beautement et al., – The Compliance Budget

[62] Gonzalez, J. J., &Sawicka, A. (2002). A framework for Human Factors in Information Security.Presented at the 2002 WSEAS International Conference on Information Security, Rio de Janeiro,2002.

[63] 2007 – Da Veiga – Information Security Culture – Assessment Instrument

Individuals are generally bad at evaluating risks of cyber threats, overestimating their rarity as well as their knowledge and control over them. Various biases contribute to this, including a false sense of familiarity with cyber threats, and viewing omissions as acceptable behaviour in uncertain circumstances.[64] Awareness and education programmes can be used to change risk perceptions[65] and teach employees how to easily carry out security tasks in a confident manner.[66]

Finally, a positively framed security programme based on openness, trust and empowerment is more likely to have a lasting impact and ensure compliance than solely relying on fear and blame.[67] For a lasting culture change, a combination of both rewards and a degree of coercion is more likely to be successful.[68] Rewards should be used to reinforce and motivate secure behaviour,[69] while parallel monitoring and sanctions may be used to increase the perceived personal costs of insecure behaviour.[70] Factors such as the perceived certainty of detection and severity of punishments can act as compliance motivators[71] while embedding compliance into the natural work flow can contribute to a strong CSC.[72]

10.1.3 The social environment

Humans are social beings that follow group norms, and it has long been known that peer pressure to conform can influence a person's behaviour. The same is true for cybersecurity behaviour. As people want to gain the approval of others, their behaviour may be seriously influenced by the perceived expectations of managers and peers. Clear cues from management regarding the place of security in the organisation, and the collective behaviours of co-workers can have a large impact on developing secure behaviour. A security culture, coupled with job satisfaction and organisational support all lead to enhanced security compliance.

Employees are also more motivated to comply with their organisation's security strategy when they believe others around them do as well.[73] Indeed, our tendency to follow the example of others in uncertain or new circumstances is a powerful social driver for behavioural change,[74] which is especially true when people can

[64] 2010 – Australian Department of Defence – Human Factors and Information Security; 2008 – West – Psychology of Security

[65] 2016 – Halevi et al – Cultural and Psychological Factors in Cybersecurity

[66] 2008 – Beautement et al – The Compliance Budget

[67] 2009b – Lacey – Understanding and Transforming Organizational Culture

[68] 2005 – van Niekerk – a holistic framework for fostering IS sub-culture in organizations

[69] 2000 – Nosworthy – Implementing Information Security in the 21st century

[70] 2008 – Beautement et al – The Compliance Budget

[71] 2009 – D'Arcy et al – User of Security Countermeasures; 2009a – Herath – Encouraging Information Security Behaviours in Organizations; S. Pahnila, M. Siponen, A. Mahmood, Employees' behavior towards is security policy compliance, Presented at 40th Hawaii International Conference on System Sciences (HICSS 07), 2007, Hawaii, USA. ; L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai, "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," Comput. Secur., vol. 39, pp. 447–459, Nov. 2013.

[72] M. a. Alnatheer, "A Conceptual Model to Understand Information Security Culture," Int. J. Soc. Sci. Humanit., vol. 4, no. 2, pp. 104–107, 2014.

[73] 2009 – Herath – Encouraging information security behaviours in organizations; E. Karahanna, D.W. Straub, N.L. Chervany, Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs, MIS Quarterly 23 (2) (1999); R.L. Thompson, C.A. Higgins, J.M. Howell, Influence of experience on personal computer utilization, Journal of Management Information Systems 11 (1) (1994); V. Venkatesh, M.G. Morris, G.B. Davis, F.D. Davis, User acceptance of information technology: toward a unified view, MIS Quarterly 27 (3) (2003); 2015 – Hong, Applying Social Psychology to Cybersecurity

[74] Cialdini, R.B. and Goldstein, N.J. Social influence: compliance and conformity. Annual Rev. of Psych. 55, 1974 (2004), 591–621. Cialdini, R.B. Influence. Harper Collins, 2009.

openly observe and discuss security behaviours with others using the same security tools.[75] Therefore, a security programme designed to incorporate sharing, interaction and security announcements can be effective in ensuring all employees take individual and collective responsibility for their security behaviours.[76, 77]

Finally, people naturally strive towards better outcomes for their community as a whole.[78] Belief that an individual's secure actions impact the overall security of the organisation is more likely to encourage such behaviour. This means that clear messages should be conveyed to employees regarding the importance of information security and the impact of their own actions in this regard.[79]

10.2 External factors

10.2.1 National cultures

National cultures can determine and influence individual's values and assumptions and so shape CSC and IT use in general. Specific values which are dictated by national culture include deference to authority, individualism vs. collectivism, the avoidance of uncertainty, and perceptions of control,[80] all of which can impact CSC development. Nationality can also influence organisational culture; for example, information security and compliance are closely intertwined in the US.[81]

National cultures can also affect the adoption, development, distribution and availability of technologies that naturally lead to differences. National differences in how people use specific technologies is also linked to their attitudes to privacy. For example, people from the United States were more willing to share information online than people from India and the UAE[82] which could shape their acceptance of CSC practices. Such differences in access to and use of technologies, in understanding of privacy or personal data, as well as view of authority, can all lead to differences in CSC.

[75] 2014 – Das – The effect of social influence of security sensitivity
[76] 2015 – Hong – Applying Social Psychology to Cybersecurity
[77] 2010 – Australian Department of Defence – Human Factors and Information Security
[78] A. Ardichvili, V. Page, T. Wentling, Motivation and barriers to participation in virtual knowledge-sharing communities of practice, Journal of Knowledge Management 7 (1) (2003); M.M. Wasko, S. Faraj., It is what one does: why people participate and help others in electronic communities of practice, Journal of Strategic Information Systems 9 (2000).
[79] 2009 – Herath – Encouraging information security behaviours in organizations
[80] 2006 – Leidner – A Review of Culture in Information Systems Research
[81] 2013 – Ashenden & Sasse – CISOs and Organisational Culture – their own worst enemy
[82] 2016 – Halevi et al – Cultural and Psychological Factors in Cybersecurity

11. Existing practices and resources

11.1 Awareness, education and communication

Knowledge, together with attitudes, values and risk perception, can all determine people's behaviours. This is important as security awareness programmes, education and training can be leveraged to influence their knowledge which, in combination with organisational culture change, can bring about a lasting CSC.

Education can be used to change security awareness[83] by teaching employees what, how and why to do things [differently], [84] and this security awareness will then foster CSC as it matures from knowledge to conviction, acceptance and behaviour.[85] The understanding of threats and available tools,[86] acceptable and unacceptable behaviour, applicable sanctions and countermeasures, as well as the underlying reasons for new security practices,[87, 88] all act to foster ownership and compliance among people. This understanding can be achieved via open, timely communication and a relevant and well-designed educational culture.

To effectively impact security awareness within an organisation, training programmes should be designed with two things in mind: (1) understanding the responsibilities attached to different functions; and (2) achieving a company-wide minimum awareness level.[89] Everyone in the organisation should receive some basic level of training, and employees should be equipped with risk awareness, skills and controls specifically related to their role. [90] To achieve secure behaviour offer employees a personalised and meaningful education to help them fulfil their responsibilities utilising a variety of interactive training to instil this new knowledge, such as games and role-playing, to facilitate engagement, participation and openness.

Designing a good awareness programme will recognise and reflect human psychology, cognitive abilities, social attitudes and modern work-environments. Programmes should afford employees autonomy, involvement, and ownership,[91] with security goals aligned to corporate motivations and organisational structures. Finally, management should set an example for the organisation by allocating sufficient resources and offering continuous guidance and support. To that end, specific, realistic and measurable goals, as well

[83] K. Alfawaz, Salahuddin and Nelson, Karen and Mohannak, "Information security culture : A Behaviour Compliance Conceptual Framework," 2010; Eminagaoglu, M., Ucar, E., and Eren, S., 2010. The positive outcomes of information security awareness training in companies – a case study. Information Security Technical Report, 4, 1–7.

[84] 2005 – van Niekerk – A holistic Framework for fostering IS sub-culture in organizations

[85] 2015 – Hewlett Packard – Awareness is only the first step

[86] 2014 – Das – The Effect of Social Influence on Security Sensitivity

[87] 2002 – Martins & Eloff – Information Security Culture

[88] Alnatheer, Understanding and Measuring Information Security Culture, 2012; Koh, K., Ruighaver, A. B., Maynard, S., & Ahmad, A. (2005). *Security Governance: Its Impact on Security Culture.*; Maynard, S., & Ruighaver, A. B. (2002). *"Evaluating IS Security Policy Development".*; Ramachandran, S., Srinivasan, V. R., & Goles, T. (2004). *Information Security Cultures of Four Professions: A Comparative Study.*; Tarimo, C. (2006). *ICT Security Readiness Chechlist for Developing Coutries: A Social-Technical Approach.*; 2015 – OECD – Digital Security Risk Management for Economic and Social prosperity

[89] 2014 – PCI Security Standards Council – Best Practices for Implementing a Security Awareness

[90] K. Thomson, R. Von Solms, and L. Louw, "Cultivating an organizational information security culture," Comput. Fraud Secur., pp. 49–50, 2006; S.Furnell and N. Clarke, "Organisational Security Culture : Embedding Security Awareness, Education and Training," no. Dti, 2005; 2005 – van Niekerk – A Holistic Framework for Fostering IS sub-culture; 2015 – OECD – Digital Security Risk Management for Economic and Social Prosperity

[91] 2004 – Schein – Organizational Culture and Leadership, p. 329.

as appropriate communications with employees are crucial to the success of any awareness programme. [92] Success factors for a good security awareness programme may be systematised in the following way: [93]

- **Stay relevant** – both with regard to new threats, as well as employee and organisational changes. All necessary knowledge for different staff should be encompassed, along with management's vision for roles and responsibilities.[94]
- **Plan for natural learning**– sufficient time should be set aside for training. The programme should positively influence the knowledge, the attitude and the behaviour of participants.[95]
- **Involve the entire organisation** – open communication and awareness throughout the organisation allows for internal consistency and feedback for improvements.
- **Share the enthusiasm -** a creative, varied and tailored education programme may achieve more.[96] Methods depend on the organisation's wishes and budget but may include one or more of games, stories, films and case studies, workshops and crisis exercises.

11.1.1 The relationship between Cyber Security Culture and Information Security Awareness

Cyber/Information Security Awareness frameworks and trainings are well established strategies for raising the cyber security resilience of employees. Security awareness can be defined as "an ongoing process of learning that is meaningful to recipients, and delivers measurable benefits to the organisation from lasting behavioural change". [97] The difference between CSC and Cyber Security Awareness is that Cyber Security Awareness is a single element or sub-set of CSC. Employee *awareness* is one element of CSC, however, CSC takes a broader and deeper view of an employee's cyber security posture, encompassing behaviours, attitudes, norms, beliefs, interactions, etc., as well as awareness.

11.2 Tools, frameworks and methodologies

A security culture transformation is complex and requires changing values and beliefs, altering behaviour, and ultimately shaping underlying assumptions regarding cybersecurity. Different approaches exist on how exactly to develop and foster a CSC. The following comprehensive framework offering a step-by-step guide to systematise the above-offered advice, has been proposed: [98]

- **Top management commitment** - as a first step, senior management should set the new direction of security culture through statements, slogans, awareness campaigns, examples, rewards and sanctions. Organisational culture will change, shaped by this commitment and reinforced through a corporate information security policy.
- **Define problem in business context** – secondly, employee attitudes and behaviours should be assessed in the context of the specific organisation.
    - **Assess the current state** – Before any further steps are taken, the current state of security culture in the organisation should be assessed whereby the existing (1) values, policies and procedures, (2) practices, (3) assumptions/beliefs, and (4) knowledge is examined.

---

[92] 2007 – Yanus, Shin – Critical Success Factors for Managing an Information Security Awareness Program
[93] 2015 – Hewlett Packard – Awareness is only the first step
[94] K. Thomson, R. Von Solms, and L. Louw, "Cultivating an organizational information security culture," Comput. Fraud Secur., pp. 49–50, 2006.
[95] Kruger, H. & Kearney, W. 2006. A prototype for assessing information security awareness. Computers & Security, 25(4), 289 – 296.
[96] L. Malandrin and T. C. M. B. Carvalho, "Maintaining Information Security in the New Technological Scenario," vol. 5, no. 3, 2013.
[97] Information Security Forum definition for information security awareness training.
[98] 2005 – van Niekerk – A Holistic Framework for Fostering IS sub-culture in organisations

- **Define the ideal state** – an ideal state for the business process should be envisioned next, defined along the same 4 lines. All these aspects should be approached with a specific and measurable goal in mind.
- **Determine the steps needed** – the steps to move from the current state to an ideal state should be clearly defined. A shift from abstract values to specific, clearly prioritized SMART goals should be made.[99] The security policy can be used here to shape future goals, processes and employee education.[100]

- **Educate the employees** – education is a key element in convincing staff of the need to change the existing security culture, teaching them what to do, how to do it and why it should be done. One should design the educational program with these goals in mind. Remember that culture changes are require time and persistence. Employees must be made aware that the current culture is no longer appropriate.
- **Define culture change metrics** – metrics should be used to measure the development of CSC and offer continuous feedback to employees and management.
- **Feedback, rewards and punishments** – Continuous feedback would be offered to employees by management through rewards and sanctions based on performance metrics.
- **Review and refinement** – the initially set goals may require revising if they are impossible to achieve or unacceptable to employees. In some cases, the final culture being strived for can be strengthened through renegotiation.

Other frameworks for developing and transforming CSC within organisations can be found in the Annexes to this report.

11.3 Measuring successful performance

Metrics have a crucial role to play in culture change and information security, as they help assess the current and desired CSC,[101] as well as any progress being made. They offer useful feedback to employees and management, and can affirm the effectiveness of security measures implemented under the new cybersecurity culture by demonstrating how successful they are. [102]

Good metrics should be quantifiable, repeatable and comparable to allow for accurate insights. They should also be easily obtainable, relevant and offer useful feedback for improvement. [103] Special attention must be paid to ensure all selected metrics are relevant for CSC. For example, metrics such as 'number of employees partaking in cybersecurity education' or 'results of questionnaires on cybersecurity knowledge and technical skills' are quantifiable and comparable and are relevant to establish the level of knowledge and awareness of employees. However, they are not sufficient for understanding CSC, as they do not relate to employee behaviour in practice, nor their attitudes and beliefs.

Employee behaviour may be examined by measuring the impact of CSC in practice. In this regard, certain cybersecurity software tools collect useful data on the number of attacks to the organisation's network, the number of prevented attacks and the time it took to recognise them. Furthermore, fake phishing and

[99] 2013 – Atoum, Otoom, Ali – A holistic cybersecurity implementation framework
[100] 2005 – Schlienger – Tool Supported Management of Information Security Culture
[101] 2005 – van Niekerk – A holistic framework for fostering IS sub-culture in organizations. Schein, E. H. (1999b). Empowerment, coercive persuasion and organizational learning: do theyconnect? The Learning Organization, 6(4), 163–172. Von Solms, B. (2000). Information security - the third wave? Computers & Security, 19(7), 615–620.
[102] 2005 – van Niekerk – a holistic framework for fostering IS sub-culture in organizations.
[103] ENISA – 2011 – Measurement Framework and Metrics for Resilient Networks and Services: Challenges and recommendations

malware attacks sent to a company's own employees may also give insight into the cybersecurity behaviour of staff. Compliance may also be measured through technical tools that monitor employee activities.

Finally, measuring of attitude and beliefs regarding cybersecurity within the organisation is also necessary, however, more difficult to quantify and compare. Questionnaires and/or communication channels may be used to study employee perceptions and understanding regarding some key aspects of CSC, including cybersecurity threats, management commitment, the availability of necessary resources, current, effective and easy-to-use technical tools and policies, individual involvement and responsibilities regarding cybersecurity, and the effectiveness and openness of communication on the matter within the organisation.[104, 105, 106, 107, 108, 109] Aspects more closely related to employee beliefs and assumptions may be also examined by looking into employees' intended activities, overall feelings and emotions about organisational security and practices, their sense of belonging, social communication and incident reporting, as well as what they perceive are the norms of organisational conduct and practices within their company.[110]

[104] 2007 – Da Veiga – Information Security Culture – Assessment Instrument

[105] 2007 – Da Veiga – Information Security Culture – Assessment Instrument; Martins & Eloff 2002

[106] 2005 – Schlienger – Tool Supported Management of Information Security Culture; Martins A. and Eloff, J.H.P (2002) Information Security Culture, In: M.A. Ghonaimy, M. T. El-Hadidi and H.K. Aslan, eds. Security in the information society, visions and perspectives, IFIP TC11, International Conference on Information Security, Cairo, Egypt, Kluwer Academic Publishers, 203 – 214.

[107] 2005 – Stanton et al – Analysis of end user security behaviors

[108] Detert, J. R., Schroeder, R. G., &Mauriel, J. J. (2000). A Framework for Linking Culture and Improvement Initiatives in Organisations. Academy of Management Review, 25(4), 850-863.

[109] 2002 – Maynard – Exploring Organisational Security Culture – Research Model

[110] Roer, K., & Petrič, G., CLTRe Indepth insights into the human factor: The 2017 Security Culture Report, 2017.

12. Recommendations

This report has described good practices, methodological tools and step by step guidance for those seeking to commence or enhance their organizations own Cybersecurity Culture programme, including resources to produce a business case to secure funding for such a programme. The success of a CSC programme rests on a number of key elements, these elements are identified and described below.

Recommendations for a successful CSC programme:

6. Secure buy-in at the highest level

Senior buy-in at the highest organizational level is essential for the success of the programme. Senior figures are needed that can to act as champions for the programme and lead by example thereby influencing the staff's behaviour towards the programme.

7. Follow the CSC Framework for the implementation of the programme

The CSC Framework presented in this report provides a process to guide the CSC programme in the form of a step by step implementation centred around specific activities, their implementation and measurement of impact.

8. Know your organization so as to ensure success

This step within the CSC Framework is key to ensuring the success of the programme, because it will inform the decision making processes that define the goals, success criteria and target audience of the CSC programme.

9. Measure the current cybersecurity level of the target audience

Calculating the current level of CSC of your target audience will assist in measuring the effect of the activities you chose to implement and thus the impact of the CSC programme.

10. Draw upon the good practices identified in this report

A number of good practices have been identified from interviews with CSC professionals within organizations across Europe and desktop research that will assist in planning and executing a successful CSC programme.

Annex A: Introduction to the interviews

Purpose/Goals

Interviews with employees of various ranks within multinational enterprises (MNEs) were conducted to verify and expand upon the academic and theoretical understanding of CSC and organisational culture change. Collecting and incorporating the knowledge and experience of people with varying levels of responsibility for cybersecurity and organisational culture, this report seeks to understand the complex interactions which take place within organisations when cultural change takes place. This analysis will contribute to assessing, understanding and developing practical guidelines, methods, and metrics, suited to invoke and promote cybersecurity culture ("CSC") within organisations.

Conducting interviews allowed for a deeper understanding of the role and function of CSC, as well as the attitudes towards it within existing organisations. Particularly, the role and interplay of different departments within complex organisational structures were examined, as well as the necessary motivation and success factors for an effective CSC programme. By incorporating the views of different stakeholders in this report we have strived to ensure the objectivity, usefulness and sustainability of our findings.

Methodology

To identify and target appropriate interviewees, a sampling strategy was developed. The strategy focused on mature organisations, be they national or multinational. The maturity of an organisation was determined, *inter alia,* by examining the presence and size of cyber or information security units within it, as well as the existence of senior functions dedicated to cybersecurity. Such organisations were deemed more likely to have developed a CSC and, therefore, were able to contribute their practical experiences and knowledge to this report. Alongside private companies, a small number of public sector organisations and academics in the field of CSC were also interviewed.

Other factors which guided the targeting of interviewees included the size of the organisation, as judged by number of employees and turnover, and the relevant industry sector, in which the companies were active. Finally, to ensure a fair geographical spread while maintaining focus on the European cybersecurity context, no more than 25% of all interviewees could come from outside Europe.

Building upon the sampling strategy, a contact list of 162 contacts was developed, identifying suitable participating organisations and persons. This contact list was comprised of existing contacts of ENISA, as well as contacts identified through desktop research - both with regard to the academic (based on Task 1), and the non-academic spheres of cybersecurity culture. Finally, a snowball approach was employed during interviews, prompting interviewees to contribute to the expansion of the contact list at their will. In this regard, we were willing to interview multiple individuals from within the same organisation, providing they performed different roles, so as to identify and assess multiple viewpoints within an organisation.

Building upon the initial scholarly research, four interview questionnaires/protocols were developed, corresponding to different groups of interviewees – (1) employees, (2) employees with CSC responsibilities, (3) senior management and (4) CSC experts/consultants. This ensured the relevance of questions to the particular experience of different interviewees. The questionnaires comprise between 19 and 32 questions, focused on identifying practices, tools, frameworks and metrics, related to developing and fostering a mature CSC, as well as exploring its benefits. The interview protocols include open and closed questions, which seek to gather qualitative data regarding CSC artefacts, interaction with different departments and

individuals, organisational dynamics in its shaping and critical success and failure factors for CSC within organisations. The questionnaires can be found in Annex C to this report.

The interview questionnaires were used to conduct 24 semi-structured interviews which lasted between 35 and 60 minutes each. The interviews were conducted virtually - through the means of a telephone, Skype or conference calls. By using a semi-structured interview, validation of findings and contribution of new information by the interviewees was possible, while contextual flexibility for each specific interview was retained.

Prior to the interviews, interviewees were sent the questions to ensure the maximum possible value was derived from the interview. Interviewees could decline to respond to any questions and upon request could review and amend the transcript of their responses to ensure their views and opinions were correctly represented.

Annex B: Breakdown of interviewees

Selection criteria and rationale

Following a targeted sampling strategy, organisations with an anticipated higher cybersecurity maturity, and people with expected CSC experience, were approached as interviewees. MNEs in particular were deemed to be suitable for our research. Due to the greater availability of resources at their disposal, as well as their higher exposure to cybersecurity threats, they were seen as more likely to have developed and invested in their cybersecurity maturity. Particularly, MNEs active in fields of IT, software development, as well as sectors dealing with sensitive data were seen as more likely to have explored CSC and invested in it, hence were approached.

The contributions offered by MNEs were deemed particularly enlightening and comprehensive. Their size and history led to vast experience regarding organisational governance, restructuring, and cultural change. This resulted in greater awareness among employees of different roles, responsibilities and the interplay between departments within complex organisational structures. Moreover, their international reach and operations meant they could have indispensable insight into the impact of national cultural differences on the CSC of a global company. Finally, regarding the geographical spread of companies, an emphasis was placed on examining CSC in a European context, however, a number of US interviewees were also approached due to the high profile of technology and cybersecurity in companies across the Atlantic.

Within organisations, three potential groups of individuals were considered for the interviews:

1. Individuals with CSC responsibilities and experience in promoting, fostering and maintaining a CSC were interviewed. These were often persons in the roles of CISOs, CIOs or CSOs, but they also included regional or departmental positions of similar responsibilities. Due to their function as liaison between different stakeholders, such individuals had first-hand detailed experience of the planning, development and implementation of CSC programmes within organisations, as well as the involvement of different departments.
2. Senior management was interviewed with a view to examine their level of involvement and commitment to cybersecurity and CSC. The role of leadership has been reiterated as a key success factor for organisational cultural change and the successful adoption and embedding of new cultural practices. Moreover, cybersecurity is increasingly a strategic issue for many organisations, necessitating the involvement of senior staff.
3. Employees were interviewed in order to examine the involvement and knowledge of staff with regard to cybersecurity, CSC, as well as their organisation's formal structures involved in cybersecurity. The quality of CSC programmes may be judged by the impact it has on employee's experiences, work, attitudes and behaviour. The involvement of employees allowed the report to examine which policies, strategies or programmes, from the employees' point of view, were most impactful.

Finally, interviews with CSC experts and consultants were planned. Drawing upon their experience with a wide range of clients and approaches to CSC, experts and consultants were approached in order to collect their guidance, general observations and conclusions regarding success and failure factors for CSC programmes. As parties, external to companies, with in-depth knowledge and wide-ranging experience in the sphere of CSC, their contributions were deemed to bring in objectivity and comprehensiveness.

Distribution of interviewees

Pursuant to our strategy, we interviewed representatives of 4 different groups of respondents. By far, the persons who most often volunteered or were proposed as interviewees for our research were those persons within the organisation who dealt with cybersecurity related issues and activities, whether approaching the issue from the technical or social sides. This resulted in most of our respondents being employees with CSC responsibilities. As the Table below shows, 18 of our 24 respondents (75%) fell in that group.

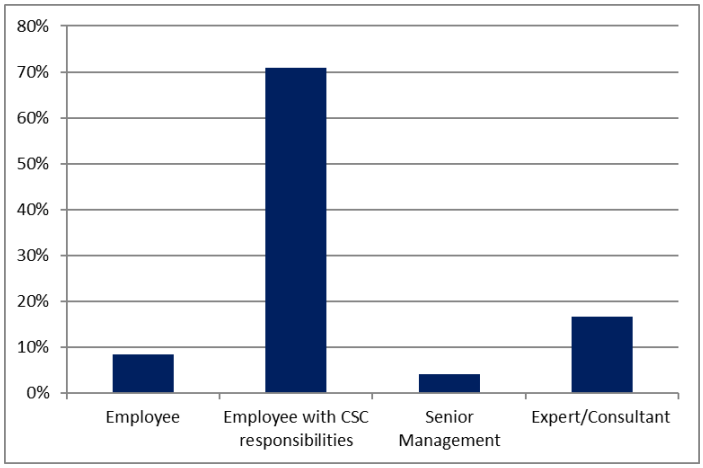

Figure 1: Type of respondent by role

We strived to conduct interviews with companies from across Europe and the world. We have assigned the nationality of a company depending on the location of its headquarters. As is visible from the table below, most of the participating companies were based in Western and Northern Europe, but we benefited from contributions from other geographical areas as well.

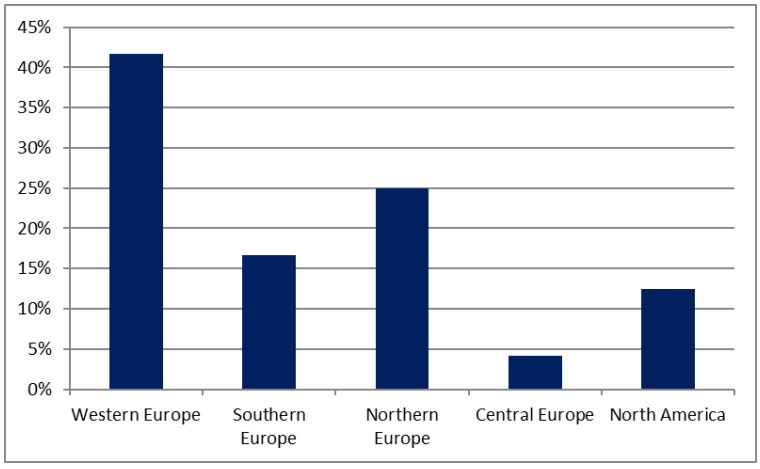

Figure 2: Geographical distribution of respondents

The respondents came from companies ranging in size, as judged based on employee numbers world-wide. There was a relatively equal split among participation from companies under and over 5,000 employees, which allowed us to incorporate the experiences of both larger and smaller organisations.

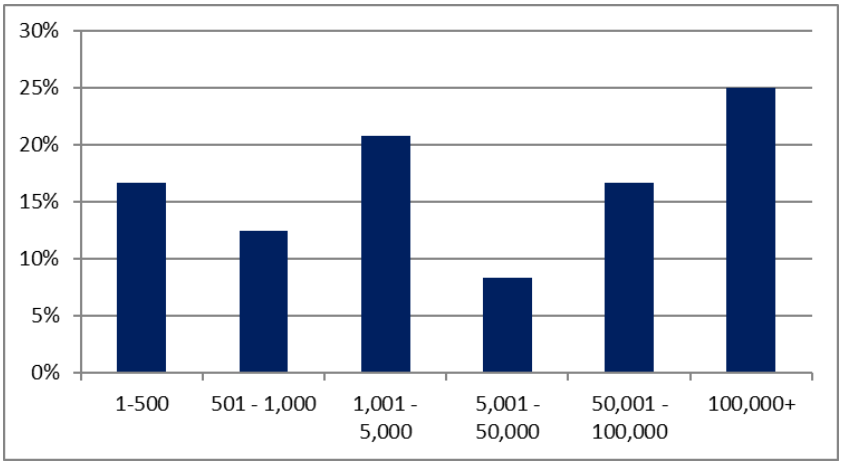

Figure 3: Size of organisation by number of employees worldwide

Interviewees came from a range of backgrounds and sectors. As expected, companies in sectors related to technology and security, as well as those dealing with sensitive information, were most likely be invested cybersecurity stakeholders and to volunteer and contribute their experiences to our research. Nevertheless, sectors such as transport, communication and professional services were also aware of and involved in cybersecurity and CSC.

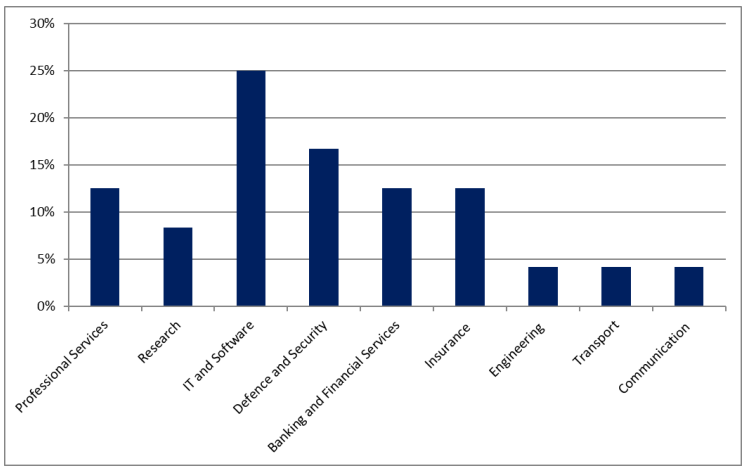

Figure 4: Type of organisation by sector

Annex C: Analysis of responses

Defining Cyber Security Culture

The definition of CSC adopted for this study is as follows:

> CYBER SECURITY CULTURE (CSC) OF ORGANIZATIONS REFERS TO THE KNOWLEDGE, BELIEFS, PERCEPTIONS, ATTITUDES, ASSUMPTIONS, NORMS AND VALUES OF PEOPLE REGARDING CYBER SECURITY AND HOW THEY MANIFEST IN PEOPLE'S BEHAVIOUR WITH INFORMATION TECHNOLOGIES

The majority of the respondents had heard of the term "Cyber Security Culture" and overall agreed with the definition provided above, though a number volunteered minor alterations to its scope which suggests the boundaries of this CSC concept have yet to be formalised. The central reason given for agreeing with the provided definition was that the notion of *culture* implies a holistic and inclusive approach to cyber security, which is necessary to achieve a change in behaviour within organisations.

CSC includes all employees and should address their needs as well as raising awareness and assisting them in making the right decisions when faced with a potential cyber threat. It suggests a robust framework, a strategy and policy, all of which work towards strengthening organisational cyber security culture on all levels.

> *"For me, I understand CSC as the risk exposure behind it and the willingness of management to address that in an entire framework, not only cyber security, but also the organisation, the processes and the IT staff behind it. It also refers to spending sufficient resources, budget, people and time."*

Those respondents who wished to amend the definition above, overall felt it was narrow. One respondent stated that it should include the requirement to understand your organisation and its needs, while others felt that the definition was too limited in that it focused on cyber security as disconnected from an overall security or information security culture.

> *"We feel that the definition of only focusing on "cyber" is too narrow. It should focus more on a holistic information security strategy. For example, not discussing confidential company information on a train or at an airport. It is not only about cyber space. We use the term cyber security but focus more on using information security."*

There is a preference for discussing cyber security in terms of "a culture" as it implies a focus on people, technology, behaviour, business processes and awareness in their day to day tasks and interaction with IT within organisations. One respondent even referred to it as CSC "way of life" and "the way in which you do things" that extends across work and into the daily lives of people, which is seen as the optimum way to strengthen protection against cyber-attacks. Culture also implies that the focus is not solely on technology and the ways in which people link with technology, but also on how they relate to each other and work together and the context within which this happens.

Culture and cybersecurity within organisations

Motivations for developing CSC

The motivation for having strong CSC is compliance to standards and regulations (especially in highly regulated sectors such as health and banking), strengthening security, and effective management of risk to the company, its business associates and clients. Reputation was also mentioned by one technology firm, which wishes to present an image of strong cyber security to its clients. A respondent from a IT security consultancy background remarked that the motivation for companies to seek outside consultancy services, was often when an awareness or training programme was seen to have failed, and that people were not paying attention to cyber security within an organisation. The focus would then be on moving toward a more holistic and inclusive way of addressing cybersecurity, employee behaviour and change.

Respondents recognised the importance of human factors and behaviour change as a defence against cybercrime, and how a holistic approach is the optimum way to ensure that everyone working within an organisation is aware of cyber security threats and how to respond to them. The interviews presented an understanding of CSC as an approach that includes people and behaviour at the centre and which allows for a deeper understanding of how technology and security is experienced and practiced in day to day working life.

The CSC approach is inclusive and a way to communicate responsibility to each member of staff to ensure awareness and caution in their daily actions.

> *"For us "cyber" is merging the information security part with the actual technology. The "culture" part means it's part of everyone's activities – it becomes part of the way you do things, look at things, part of your behaviour. It has to be in the business process and in your behaviour as an employee. We don't only expect our employees to behave in a secure manner as employees, but we expect them to also bring those aspects in the way they do business."*

For one respondent, the concept of a culture also indicates that cyber security awareness should extend into people's home life as the boundary between home and work are increasingly being eroded:

> *"It's not just your job. Our jobs and our lives bleed over, cross from one to the other. Whether it's a person who works from home, looks at their email, looks at the cameras on their door because their doorbell just ran, even just surfing the web. There is little distinction between home and work in most people's lives today."*

The focus on taking a holistic approach to cyber security is to ensure that the likelihood of a "weak link" within an organisation is diminished, thus responsibility for maintaining a secure atmosphere is overall presented as collective endeavour, where every staff member contributes to a united front against cybercrime.

CSC resources (cybersecurity policies and strategies)

While a cyber security strategy lays out the long-term plans for cyber security and is developed and supported at the higher levels of each organisation, a cyber security policy details the roles, responsibilities and hierarchies when it comes to implementing cyber security on a day to day basis. It also details what the responsibilities of each member of staff are regarding cyber security, as well as broader security such as physical, information security and data protection and privacy. The company policies are presented to all new staff and kept easily accessible, usually on the company intranet. All new staff may need to sign to

display understanding, recognition and compliance to company policies and these may be used should a matter of negligence or non-compliance come up during a staff members time with the company.

With regard to updates to strategies and policies, and communication of these updates, in most instances there is a regular update cycle, usually once a year where these documents are re-visited and updated. Respondents also stressed the need to leave room for ad-hoc updates, usually to respond to urgent changes in the threat landscape or any new technologies or approaches that are being implemented internally.

> *"We are informed via e-mail and newsletter. It is a general newsletter with a warning. Normally it's from the CEO or another senior management. It depends how often the newsletter comes up. It could also be Communication Managing Partners, and emails could also be from the CEO, depending on the severity of the message."*

For many of our respondents this flexibility was important as cyber security is an ever-evolving landscape, which requires up-to-date policy. Regarding the communication of changes, these are usually presented in internal newsletters, emails or on the organisation intranet, depending on the nature of changes. Minor changes tended to be communicated during other company communication from the communication department while major changes are sent out specifically and usually from the CEO or CSO.

The importance of embedding cyber security policies and procedures within broader organisational policies was stressed by one of our respondents, which made an example out of CEO fraud. This entails a fake email sent to a member of staff in the finance department. The email appears to come from the CEO and requests an urgent transfer of funds, directed to the cyber criminal's account. In our respondent's view, a strong cyber security policy will not work to prevent this type of fraud being successful. A strong policy on processes, which dictates the steps necessary for allowing a transfer of funds and the CEO relationship with the finance department, would be necessary; and even then, compliance with these processes would require the appropriate organisational CSC.

Management involvement

It was stressed by all respondents that in order to build a strong SCS within an organisation it was imperative to get support and buy-in from senior management. When asked about senior and middle management involvement in the development and implementation of cyber security we found that the degree to which management (senior and middle) are involved in the development and implementation of CSC depends on the company structure and where cyber security policy and strategy sit within that structure.

In practice, these two groups are involved in different ways:

Senior management CSC implementers interviewed for this study were unanimous in identifying that senior management are essential for the success of a CSC as they hold the overall strategy formation of each organisation and are responsible for financial decision making. The initiation of a CSC thus starts with convincing them of its importance, getting their approval and also a dedicated budget. Senior management is also seen as imperative in further developing CS strategy and communicating it down the chain of command. Members of senior management need to be role models and champions for CSC, and lead by a strong example. The responsibility for the overall company direction and agenda setting also lies with the senior management and the

> *"They [senior management] are very involved, because if their employee screws up the manager is equally accountable for what happened. So, there is an incentive there, you want to keep your job. For example, if [City] has a lab where the cause of a cyber security incident emerged, then that is a red card against the entire lab. If you get enough red cards, then [the Company] will*

shut down that lab. Issues like this get executive attention and the executive would need you explain how this happened and what they are doing to correct it, and it better not happen again."

Middle management involvement is also seen as important. Not only can they initiate a CSC programme but they are often the management level in day-to-day contact with employees. Hence, they represent an important mechanism for reviewing and giving feedback on any policies and communicating them downstream to respective teams and staff members. Middle management should also be empowered to communicate any issues upstream to ensure that senior management is aware of any problems or barriers that may arise to the implementation of CS policies. Middle management are also be responsible for oversight and ensuring staff compliance.

"Buy in from executive management is very important [and so] is buy in from middle management. You get the go ahead from the executive management but the message will get stuck in middle management if you don´t have their buy in."

Responsibility for CSC

Perceived responsibility for CSC is influenced by multiple factors, ranging from differences in national cultures reflected in how people respond to cyber threats and security policies, through to the internal structuring of organisations and the assigning of cyber responsibilities. On the assigning of responsibilities, all but one of the respondents agreed that cyber security should be presented as a collective contribution, where each staff member contributes to the overall safety of the organisation. While responsibility for (i) drawing up policies and procedures, (ii) providing guidance, (iii) setting the overall company cyber security stance, and (iv) CSC delivery, are seen as the responsibility of both upper management and the technical teams, the compliance and following of protocol is seen as the responsibility of every member of staff.

"In most communications, the message used is that the security of all of us depends on the security of each of us. So, the overall security of the company requires each individual to be aware of new attacks. So, I would say it is presented as a collective responsibility but where each person has their own role in this process."

This message is delivered through a variety of channels, and there is an understanding among respondents that for this to be realised, communication to employees that is tailored to be relevant to them and their role is imperative. CS should be supported by easy-to-use tools and include feedback and positive reinforcement to ensure employee participation on all levels. While such personal communication is viewed as a very effective tactic, it was acknowledged that achieving this is challenging for large organisations with many employees.

Two consultants made interesting comments on this trend and noted that staff may feel anger at the responsibility placed on their shoulders when they felt that they were doing an otherwise good job in their role, but risked being sanctioned for a mistake with regard to cyber security threats, which are becoming increasingly sophisticated. Furthermore, cyber security might still be seen as a technological issue first and foremost and thus the responsibility of the IT department, which is viewed as the primary line of defence as they have the right tools and knowledge to fend off cyber security threats.

For staff whose work does not entail heavy IT use and who may lack IT skills, there was a view expressed that it is, to some extent, unfair to expect high levels of cyber security awareness from these individuals. As cyber criminals are often perceived (correctly or incorrectly) to possess high IT and/or social-engineering skills, this is seen as an unfair fight.

"So, on one hand we have people who don't understand the technology and then we have really capable and skilful cyber criminals. It is their job to create cyber-attacks, phishing emails etc. It is very naïve to think that we can teach the employees to protect themselves from these criminals – the skill gap is too large."

It is therefore important that the focus is not shifted entirely on to employees and that technological means are also fully utilised to improve the cybercrime protection and resilience of systems and networks. An example would be to divide up large organisational networks, so that once ransom or malware has infected one computer it is not spread throughout the entire network. That said, even critical security controls like network segregation have variable effectiveness against attackers, and there are risks involved in users placing over-reliance on technological controls.

It was stressed by respondents that forcing cumbersome policies on to employees, would have the likely effect of staff rebelling and choosing to ignore any training or cyber security awareness attempts. Care should be taken to develop policies and practices in cooperation with employees and listen to their feedback and also learn about the specificities of their roles and day-to-day working lives. Embedding CSC in already established practices, is more likely to succeed than forcing an entirely new set of practices on employees, as this will cause delays with their work and create a resistant attitude towards change.

Training and awareness programmes

All the organisations offer some form of cyber security training and awareness programmes. All but one respondent called their approach a programme, while the one referred to it as "teaching new staff about our procedures, including cyber security".

Regarding training, the most common approach is to offer all staff the same basic level of training (most often in an online learning environment) and then offer dedicated training to specific target groups. This applies to individuals, departments or teams that are seen to be faced with specific cyber security challenges or are seen to be targeted specifically by cyber criminals. This can for example be aimed at those who work in the financial department or those working with personal data. A suggestion is to focus on risk based training for specific groups to ensure that they get fit for purpose and relevant information about potential cyber threats aimed at them.

"Most of the training is the same for everyone, not customised. But we have different trainings that are more relevant for different positions. We have some longer trainings and the shorter ones are on specific subjects. For example, last year we had a training called "privacy-by-design" for those who build and maintain systems, regarding the things they should consider regarding privacy. Not just how the tool works, but also how to keep the data inside it safe. I can definitely see us coming up with several different trainings specific to that over the next year (with GDPR coming up). We have been working on the GDPR for a year already."

All new staff must take the cyber security training as part of induction and then re-take the training at specific intervals (usually once a year) to ensure they are still proficient and up to date. Training programmes are in most instances conducted online but a variety of tools are used for training purposes.

"We attempt to raise cyber security awareness among our employees to let them understand how they can be targeted or react to cyber security situations in their daily life. Who are the main contact points, the roles and positions in [company] that can help them or that they can refer to, when they feel uncomfortable with a specific situation that may lead to a cyber-attack."

Awareness programmes are held within all organisations and variety of tools are used to reach and engage with employees. The awareness programme is an addition to the training programme, and is meant to keep employees engaged with the issue of cyber security. Awareness raising is seen as an on-going programme, which is important to maintaining a strong CSC. Organisations use a variety of tools to raise awareness, ranging from training, emails, information sections on the organisation intranet, posters and flyers, through to more direct engagement through games and events (e.g., hackathons and seminars) and providing internal certifications and merchandise (e.g. mouse pads, etc.) to staff who have completed security training. One organisation dedicates a whole week to the issue of security (which includes a focus on cyber security as well) whereby the aim is "to really shake everyone up a bit".

CSC communication and promotion

To build a strong CSC within organisations, and change behaviour, it is of key importance to reach and engage with staff on all levels, through a variety of medium. The majority of organisations use a number of different instruments and approaches to inform and train their staff about cyber security threats and activities. Many respondents favour interactive and engaging approaches, such as games, videos and exhibitions but also rely on more 'traditional' ways of communicating such as posters, emails, flyers and seminars.

> *"Almost every year we do posters and we send them out to our offices. Stories, we sometimes give awards and we would highlight individuals within the company that have made a really great choice or decision that led to us being more safe [sic.]. We will use that to promote them and cyber security. Look at Person X, who did XYZ."*

Organisations host events, which may be around a specific type of threat (e.g., WannaCry) or more general cybersecurity awareness topics. Face-to-face events were seen to be of great benefit, as these allowed employees to ask questions, give feedback and learn in an interactive two-way environment.

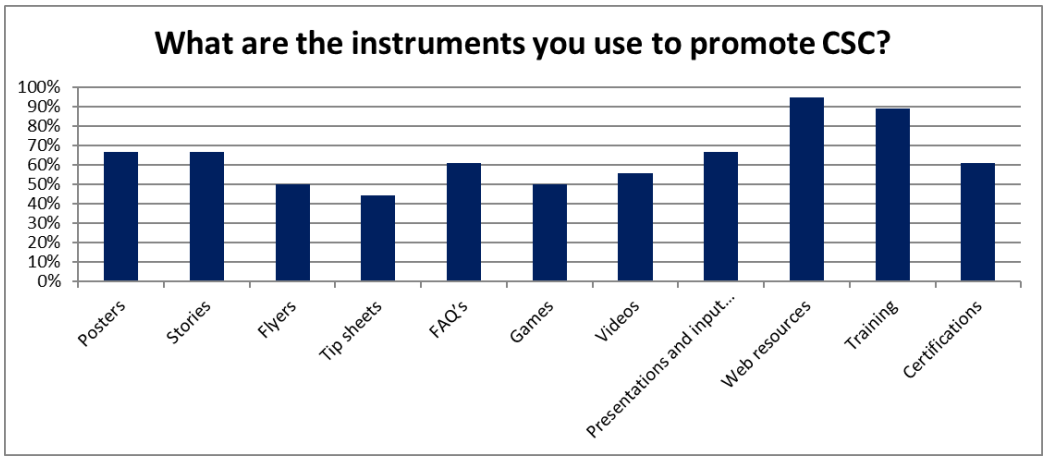

Figure 5: CSC intervention delivery methods

Stories of good practice were mentioned especially as a good way to promote cyber security through telling staff about specific security incidents, and how someone had successfully responded. These can be external incidents or internal best practice stories. A respondent from a large financial organisation explained their unique training approach, which is extended to include the families of employees to strengthen the message.

Unique Approach to Raising Awareness of CS

"One specific training we do which is quite unique is that we train the family and kids of the families in awareness in general terms, like avoiding phishing, cyber bullying, cyber gooming, sexting. We educate the kids of the employees, at the same time the parents. employee and spouse are also traIned in a different session in specific things - they are told exactly what their kids are being taught so that they are aware. The take up is high - we have to run extra sessions as everyone wants to get into this - it has been embraced by all the employees and they do ask a lot to be included in future sessions, so [this] is very successful"

Current CSC satisfaction levels

Overall, the respondents (both general employees and employees with CSC responsibilities were satisfied with the current state of affairs and progress made in developing a CSC within their organisation. However, they all explained that this was an on-going task, as the threat landscape as well as ICT was developing rapidly. Therefore, it was imperative to keep training and awareness programmes, as well as policies and strategies updated.

> *"Yes, I am satisfied with the level we have achieved but there are still huge grounds for improvement as well. Behaviour isn´t something static, you have to work with it continuously. Same must go for rules as the context changes."*

Those organisations who are in the early stages of implementing CSC, recognise that culture and behaviour change do not happen overnight, and require long-term commitment and on-going efforts to develop a strong culture. Those who displayed dissatisfaction reported that (a) there was a lack of relative skills in the employment market, and (b) that funding for awareness and training was too low, and while senior and executive levels took the issue seriously the funding did not reflect that. This highlights the importance of a strong and dedicated budget for both the initiation and continuing development of a strong CSC within organisations.

Establishing a Cyber Security Culture

Respondents with first-hand experience in establishing and implementing CSC programmes were asked questions designed to extract and distil this knowledge, so that it in the following Chapter X it can be shaped into concrete actions and guidance for other organisations to employ within their own CSC activities. These questions focused on: assembling the optimal CSC implementation/support team; the steps involved in designing and conducting CSC interventions; metrics for measuring success; recommended actions for maximising the success of CSC interventions, as well as actions to avoid.

Essential components of a successful CSC team

When asked about the ideal composition of the team setting up CSC within an organisation, all respondents claimed that broad involvement was necessary to achieve success in strategy and policy formation, implementation, training and awareness raising. Included in the question was the following list of key roles, and respondents were asked to select which ones needed to be involved and for an elaboration on their choice.

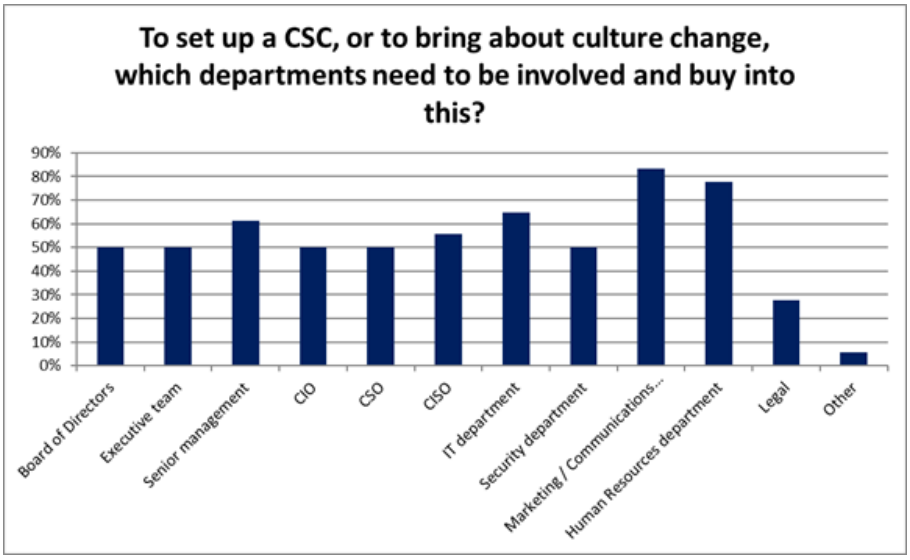

Figure 6: Assembling a CSC team within an organisation

While arguing for a broad and inclusive approach, respondents outlined that each role/department would serve a different role within the CSC team:

> *"I think they all need to be included. I think there is an implicit challenge here which is to what extent this is an external culture you are pushing on to an organisation and to what extent are you nurturing what you have already got. […] So, I think all of these departments and all the others have a big role to play here, and it's around how they listen to each other and work out what the core values are within the organisation, and understanding how the information flow and production and protection occurs within the organisation and fits within these key values "*

Board of directors, executive team, senior management (CEO, COO, CFO): The role of the senior team of the organisation is mainly presented as threefold:

- Supporting the CSC team through allocation of resources (both human resources and financial resources) and gives the go ahead. Overseeing and advising on the on-going focus on CSC.
- Formation of strategy in line with overall organisation strategy and putting CS visibly on the company agenda. CEO and board of directors set the tone for the values and goals of the organisation.
- Support the drafting of CS policies and communication of these downstream.

IT departments (CIO): IT department will have a key role in bringing to the table an in-depth knowledge of the organisation's technology and information assets, cyber threats, and technical ways to protect against cybercrime.

Security (CSO, CISO, CERT): to ensure that CSC fits within the overall security strategy and policy of the organisation. Security will bring knowledge of physical security of the organisation´s assets and information regarding access control.

HR and legal department: Supporting role in the sense that they are not involved in strategy or policy formation. HR department will assist with organising training and with employee facing issues. HR will know what can be requested of staff (legal department will also have input here), knowledge of different roles and responsibilities within each organisation. HR may also have experience with staff training and the design of training programmes. Legal department (which may be closely linked to HR) will advise on legal procedures

such as when discussing monitoring devices and networks, they can advise on the legality of any such activities and ensure compliance with law and regulation.

Communication and marketing department: Act in a supporting role and will advise on the communication of any CSC information and material. They bring the knowledge of how to target different audiences within an organisation and how to translate complex technical information into easily accessible and implementable steps**.**

Elements of a CSC framework

To enable the discussion with respondents on what a framework for establishing and maintaining a strong CSC should contain, we suggested a framework that consisted of pre-treatment phases, a treatment phase and a post-treatment phase, based on existing literature. While many of the organisations interviewed were not employing a formal framework for their CSC interventions, overall the respondents agreed with this basic structure the addition of a number of comments/steps. It was stressed that this is an iterative process whereby CSC programmes are constantly being assessed and improved. Indeed, many of the respondents commented that it would be more useful to think of this as a cycle rather than a linear process, as behaviour change and CSC formation/maintenance are on-going tasks. It was also stressed that the first step in any CSC programme must entail developing a clear understanding of the needs and conflicting pressures that apply to each of your different business units.

Metrics for measuring success

All of our respondents carry out activities to measure cyber security culture within their organisations. Overall there is a recognition that these may not entirely capture the state of affairs within the organisation, as measuring culture is a complex undertaking and uncertainty surrounding relevant KPIs is high. A work to better define KPIs and methods of measurements is ongoing within many organisations and respondents reflected on the usefulness of using ISO 27001 or 31000 and risk assessment frameworks and standards (e.g., IRAM2) as guidelines to set up their organisation-relevant metrics. The following are approaches in which the state of cyber security was measured within the respondent's organisations:

- **Technology reporting** including reports from servers and IT security tools, e.g. number of attacks and number of breeches that are picked up from IT security and antivirus software.
- **Training completion statistics** including counting how many people attended awareness or training events, or how many employees successfully completed the organisation´s online training programme.
- **Sending out surveys** with questions to employees regarding their cyber security awareness. These consist of either qualitative or quantitative questionnaires, or a mix of both
- **Security reporting data** such as the number of devices reported as lost/stolen
- **Sending out phishing emails** and malware campaigns to measure employee response, e.g., how many people "click the link".
- **Monitoring employee IT activities** in general, whilst recognising boundaries of privacy. Focus here might be more on a team or department level to avoid focusing surveillance on specific individuals.

As with the development of cyber security training, awareness and culture, respondents recognised that KPIs and metrics needed to be relevant to each organisation and their security goals and that work was either ongoing or needed to be carried out to better define these.

> *"You need to define success. You find the current situation and define a goal, and then you measure before and after to see how your programme worked and how close to your goal you have come. How you can do the measuring will be determined by what systems are in place in*

your organisation for gathering the requisite data […] In my experience counting the number of people who have completed an online training is just counting people - it doesn't tell you anything about the cyber security culture or security behaviours we want them to have."

Identified actions for maximising CSC success

When asked to recommend specific actions to strengthen the likelihood of a successful CSC, the respondents' responses fell within five broad themes:

Senior management support was mentioned throughout the interviews as an important factor of setting up, and maintaining a strong CSC. It was recognised that garnering support might involve work that included some pre-metrics to establish and communicate the state of affairs within the organisation. One respondent suggested simulation of a cyber-attack to create awareness, while another one suggested a "crash course" for management so that they would get up to speed and understand the importance of the risk to the business. Senior management should also be champions of cyber security and act as role models by following the cyber security practices implemented by the organisation, and commenting on them in way that is highly visible to the employees. Senior management also holds the power over any potential cyber security budget and potential budget increases, so it is imperative to have their full buy-in from the start. As one of our respondents stated: *"Don´t waste time doing it on your own, get support from the top. Get the expertise from the right people. It is a zero-sum game and you need 100% results."*

"Keep it simple" and "start small" was a consistent message throughout. By attempting to "catch some low hanging fruit" first, progress and impact could quickly be established and communicated to management to ensure on-going and preferably increased funding and support for cyber security culture and awareness development. Also, by starting small, would increase likelihood of success for a small IT department or an individual who initiated the turn to CSC. Starting with basic solutions allow for a low-cost initiation that can later be modified to fit each organisation was also recommended by one respondent. It was recognised that these "off-the-shelf" solutions might not appeal to employees as they are not fitted to their practise or contexts, but this would be a way to get started and gather momentum. Any successes could then be measured and presented up to senior management to justify higher spending on cyber security awareness raising programmes.

CSC is about people. The success of your CSC depends on the people within the organisation was a message that came throughout the interviews. Respondents thus stressed that communication was key and as an implementer you would need to listen to people as they communicated regarding the challenges and specificities of their role regarding adhering to cyber-security policies and adopting specific practices. "You need to make sure that people understand why they personally need to care about security", make it clear that cyber security incidents affect their jobs directly as they may cause delay, limited access, missed deadlines and loss of data, to name a few. You also need to make sure that people understand the interconnectedness between themselves and others in the organisation and that if they act irresponsibly, this may affect other people, and even put the whole organisation at risk. Demonstrate clearly the benefits of having a strong cyber security awareness, and how it may affect their personal lives as well as working lives, as this will garner stronger support amongst employees. New practices and new roles cannot be too burdensome, they need to fit into the already established roles. They should not feel like a cumbersome addition to their already established role. Hence it is important that employees are listened to and that any solutions fits around the employees but not the other way around

The importance of metrics was stressed by respondents, especially pre-metrics in the first stages of setting up a CSC as these would help with tracking successes of the implemented approach. This was identified as a key tool to convince senior management of the benefits of having a strong CSC, which would help with on-

going support of the scheme and to increase funding. Stories of success were also mentioned to drive support from other employees within the organisation. The following chapter provides good practices and guidance on forming/using metrics.

The importance of supportive IT infrastructure and technology to assist employees in taking on responsibility for cyber security was stressed by some respondents, who explained that technological tools need to be easy to use. Any solutions that are perceived to be too complex and burdensome, ran the risk of being resisted or ignored. It would also be perceived as unfair that people took on the responsibility for security, while IT systems were unsafe from a technological standpoint. IT systems should make compliance to the rules easier, not harder.

Identified action to avoid for maximising CSC success

When asked about known mistakes or pitfalls to avoid when developing or maintaining a CSC, respondents´ answers corresponded to a great extent to their recommendations for actions to follow listed in 3.3.6 above.

Don't go it alone but get definitive buy in from senior management and get employees to work within you. This will happen through engagement and a clear statement of the cyber-security issues that the organisation is faced with.

Be methodical and take it step by step. Especially when initiating a turn towards CSC within an organisation, it is important to take it slowly and work towards incorporating feedback from employees and gauge their response. Don´t expect immediate results, implementing a CSC within an organisation is a long-term project and shaping the culture to change behaviour will be an on-going process.

Work with people. Respondents stressed that surprising people with new procedures and practices, overload of information and overstatement of cyber security risks "out there" would be likely to result in resistance from employees. It was also made clear that avoiding placing the sole responsibility on employees and taking up strict sanctions, without clearly communicating roles and responsibilities would run into the same risks. Cyber-security should not be experienced as a barrier by employees, rather a tool to help them do their work. A "blame game" should be avoided at all cost – it is the role of the IT security department/staff to ensure that the people have the right tools and knowledge to change their behaviour.

Don't rely solely on eMedia to communicate cyber security awareness. eLearning is good approach, especially when mixed with more engaging and interactive approaches such as events, seminars and other face-to-face methods. This will also allow employees to feedback and ask questions, which will be useful for the development of CSC, going forward.

Compliance with internal cybersecurity rules and policies

Ensuring compliance with policies and procedures

Regarding compliance measures, majority of respondents mentioned the use of sanctions for CS non-compliance or negligence from staff. To a much lesser extent issue of feedback or positive reinforcement was mentioned. Also, when discussion sanctions, these were discussed in the broader context of compliance to company policies overall and the response follows the same discipline model as other non-compliance.

> *"There are also sanctions in place. We have just updated what we call our Progressive Discipline Policy. This has been ongoing. There's a lot of work with HR and Legal. We have put things in place that say "if you took some action that was not in line with our policy, we will inform your manager, will make a note of it for your record". Not just any bad thing, but if it's something that*

is malicious and put the company or customers' data in jeopardy, there will be a negative consequence. If it happens more than once, then it will be treated even more seriously up until termination. If it's something very egregious and malicious, it might be just that one time and your employment can be terminated. If it's a lesser offence, HR can make a note of it, sit down with you, give you more training."

When respondents mentioned positive reinforcement or feedback, respondents recognised the benefits of these approaches and two organisations said they were working on implementing this to a greater extent. When feedback is given, this is usually on the organisation intranet and is presented to all employees, and one organisation offers specific positive feedback to those who "have made a big contribution" to cyber security. Continuous feedback is also sometimes offered on the department level, where they are presented with results of metrics from risk reviews and security incidents that have occurred.

Reporting cyber threats

Respondents agreed that the reporting of cyber threats or of actions that could potential cause a cyber incident should be as easy to report as possible. Respondents stressed that it was vital to encourage people to report rather than not, and also to implement a safe and non-punishment culture for those who report. People should be allowed to make a mistake and should be corrected and awarded rather than punished for making a report. The procedure for reporting an incident should be clearly laid out and known by each member of staff. The organisations reported a number of ways in which reporting is handled.

- **Reporting through an organisational structure**, e.g., reporting to one´s line manager who will follow the report further up the chain. One respondent recognised that his is the preferred way, of reporting to a person rather than going through a complex process of officially reporting and "opening a case".
- **Reporting through a service desk,** cyber security centre or another centralised body that serves this function. Contact details for these are well presented in company intranets and are easy to find. Depending on the size of the organisation, these may be open 24/7 serving multiple countries.
- **Automated and technological ways of managing CS incidents**. Respondents reported that in many instances computers are monitored and the IT department are alerted automatically when a security incident takes place, e.g., when a malicious link is clicked or when a user visits potentially risky website.

Annex D: Pervasive themes

To conclude the analysis of interviewee responses, presented below are five pervasive themes that appeared repeatedly throughout the interviews.

- The strength of implementing a Cyber Security Culture approach to defend an organisation against cyber-crime is seen to stem from its holistic, flexible and pervasive qualities. Using a cultural approach puts the focus on people, their practices and relationships within a specific organisation's context. Respondents understand CSC as formed within each organisation, and due to its flexibility, it is able to serve the organisation better than other approaches that may be too technologically focused, or too off-the-shelf to be fit for purpose. In order to form a strong CSC, knowledge of the organisation (its people, assets, values, organisational culture, strengths and weaknesses) is imperative. Thus, an initial mapping of each organisation of should always be carried out in the beginning stages of CSC formation.

- Senior management buy-in and support is imperative for a successful SCS initiation, implementation and maintenance. Senior management will at the start agree the agenda and ensure that the CS strategy and policy is in line with the overall organisation strategy. As the CSC progresses, it is imperative that they continue to visibly support the approach, and act as CS role models. Important CS notices should be sent from senior management to enhance their gravitas and validity. Middle management is also important, as it sits closer to employees and can communicate CS messages down and up the chain. Middle managers are also important for oversight and ensuring that staff have the tools they require.

- CSC involves everyone within the organisation. Every staff member is responsible for their CS practices and it is important that this is encouraged through positive re-enforcement, and that people are provided with the right tools and training to comply with CS policies and make safe and security choices in their day-to-day work. CSC should be embedded in people´s daily tasks, they should not be cumbersome, overly complex or hinder work progress.

- Consistent training, awareness and promotion are needed to build a strong CSC as engagement with employees will ensure their informed participation in building robust defences against cybercrime. Training, awareness and promotion activities should ideally be varied, and range from email campaigns to events, which could include external speakers, training for the whole family or a focus on a specific risk to name a few examples that were presented in the interviews. Inclusive training, promotion and awareness raising will help solidify a strong CSC. Care should be taken to not overstate risk, nor communicate excessively, as this can contribute to a dismissal from employees.

- Use of standards and other documents have helped with drafting of strategy, policy, frameworks, metrics and training. Respondents reported having used a number of different documents to assist them with the above work. Using guidelines from standards or other Cyber Security documentation, can help with drafting organisational CS strategy and policy that is informed by best practice.

Annex E: Bibliography/References

Abawajy, J., 'User preference of cyber security awareness delivery methods, Behaviour and information technology', Vol. 33, No 3, 2014, pp. 237-248.

Albrechtsen, E., & Hovden, J., 'Improving information security awareness and behaviour through dialogue, participation and collective reflection. An Intervention Study', Computer and Security, Vol. 29, No 4, pp. 432–445.

Alfawaz, S., Nelson, K., Mohannak, K., 'Information security culture: A Behaviour Compliance Conceptual Framework', 8th Australasian Information Security Conference, Brisbane, Australia, 2010.

Alnatheer, M., 'A Conceptual Model to Understand Information Security Culture', Int. J. Soc. Sci. Humanit., Vol. 4, No 2, 2014, pp. 104–107.

Alnatheer, M., Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia, 2012.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. & Xu, L., 'Gender difference and employees' cybersecurity behaviors', Computers in Human Behavior, 2017.

Ardichvili, A., Page, V., & Wentling, T., 'Motivation and barriers to participation in virtual knowledge-sharing communities of practice', Journal of Knowledge Management, Vol. 7, No 1, 2003.

Argyris, C., & Schön, D., Organizational learning, Addison-Wesley, Reading, 1978.

Asch, S., 'Studies of independence and conformity: A minority of one against a unanimous majority', Psychological monographs: General and applied, Vol. 70, No 9, 1956, pp. 1-70.

Ashenden, D., 'Information Security management: A human challenge?' Information Security Technology Report, Vol. 13, No 4, 2008, pp. 195-201.

Ashenden, D., & Sasse, A., 'CISOs and Organisational Change: Their Own Worst Enemy?', Computers & Security, Elsevier, 2013.

Atoum, I., Otoom, A., & Ali, A., 'A holistic cyber security implementation framework', Information Management & Computer Security, Vol. 22, No 3, 2014, pp. 251-264.

Australian Department of Defence, Human Factors and Information Security, no date.

Beautement, A., Sasse, A., & Wonham, M., The Compliance Budget: Managing Security Behaviour in Organisations, 2008.

Business Software Alliance, Information Security Governance, 2013.

Cheng, Y., Li, W., Holm, E., & Zhai, Q., 'Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory', Computer Security, Vol. 39, 2013, pp. 447–459.

Chipperfield, C., & Furnell, S., 'From security policy to practice: Sending the right messages', Computer Fraud Security, Vol. 2010, No 3, 2010, pp. 13–19.

CISCO, Cybersecurity Management Program, 2017.

Cook, S., & Yanow, D., 'Culture and organizational learning'. Journal of Management Inquiry, Vol. 2, No 4, 1993, pp. 373–390.

D'Arcy, J., Hovav, A., & Galletta, D., 'User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach', Information Systems Research, Vol. 20, No 1, 2009, pp. 79-98.

Das, S., Kim, T., Dabbish, L., & Hong, J., The Effect of Social Influence on Security Sensitivity, Symposium on Usable Privacy and Security (SOUPS), Menlo Park 2014.

Da Veiga, Information Security Culture Assessments, 2014.

Deal, T., & Kennedy, A., Corporate cultures, Addison-Wesley, Reading, 1982.

Deal, T., & Kennedy, A., The new corporate cultures, Perseus, New York, 1999.

Denison, D., Corporate Culture and Organizational Effectiveness, Wiley, New York, 1990.

Deloitte, Risk Intelligent governance in the age of cyber threats, 2012.

Detert, J., Schroeder, R., & Mauriel, J., 'A Framework for Linking Culture and Improvement Initiatives in Organisations'. Academy of Management Review, Vol. 25, No 4, 2000, pp. 850-863.

Dimensional Research, Trends in Security Framework Adoption, 2016.

Dodge, R., Carver, C., & Ferguson, A.J., 'Phishing for User Security Awareness', Computers and Security, Vol. 26, 2007, pp. 73-80.

Dojkovski, S., Lichtenstein, S., & Warren, M., Fostering information security culture in small and medium size enterprises: an interpretive study in Australia, in Proceedings of the 15th European Conference on Information Systems, University of St. Gallen, St. Gallen, 2007, pp. 1560-1571.

Earnst & Young, Cyber Program Management, 2014.

Eminagaoglu, M., Ucar, E., & Eren, S., 'The positive outcomes of information security awareness training in companies – a case study'. Information Security Technical Report, Vol. 4, 2010, pp. 1–7.

ENISA, Measurement Framework and Metrics for Resilient Networks and Services: Challenges and recommendations, 2011.

ENISA, Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures, 2016.

Fagerström, A., Creating, Maintaining and Managing an Information Security Culture, 2013.

Fitzgerald, T., Building Management Commitment through Security Councils, or Security Council Critical Success Factors, In H. F. Tipton (Ed.), Information Security Management Handbook, Auerbach Publications, Hoboken, 2007, pp. 105-121.

Foley & Lardner LLP, Taking Control of Cybersecurity, 2015.

Furnell, S., A Conceptual Model for Cultivating an Information Security Culture, 2015.

Furnell, S., & Clarke, N., Organisational Security Culture: Embedding Security Awareness, Education and Training, 2005.

Furnell, S., & Thomson, K., 'From culture to disobedience: Recognising the varying user acceptance of IT security', Computer Fraud Security, Vol. 2009, No 2, 1999, pp. 5–10.

Geertz, C., The interpretation of cultures, Basic Books, New York, 1973.

Goffman, E., The presentation of self in everyday life, Doubleday, New York, 1959.

Goffman, E., Interaction ritual, Hawthorne, Aldine, 1967.

Greene, G., & Arcy, J., 'Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance', 2010, pp. 1–8.

Halevi, T., et al., 'Cultural and Psychological Factors in Cyber-Security', iiWAS '16, November, 2016.

Hearth, T., & Rao., 'Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness', Decision Support Systems, Vol. 47, No 2, 2009a, pp. 154-165.

Hearth, T., & Rao, H., 'Protection motivation and deterrence: a framework for security policy compliance inorganizations', European Journal of Information Systems, Vol. 18, No 2, 2009b, pp. 106-125.

Henderson, R., & Clark, K., 'Architectural innovation: The reconfiguration of existing product technologies and the failure of established firms'. Administrative Science Quarterly, Vol. 35, 1990, pp. 9–30.

Herley, C., 'More is not the answer', IEEE Security & Privacy, Vol. 12, No 1, 2014, pp. 14-19.

Hewlett Packard, Awareness is only the first step, 2015.

Homans, G., The human group, Harcourt Brace Jovanovich, New York, 1950.

Hong, J., Das, S., Kim, T., Dabbish, L., Social Cybersecurity: Applying Social Psychology to Cybersecurity, Human Computer Interaction Institute, Carnegie Mellon University, 2015.

IBM, X-Force Threat Intelligence Index, 2017.

ISC, Global Information Security Workforce Study, 2015.

Ifinedo, P. 'Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory'. Computers & Security, Vol. 31, No 1, 2012, pp. 83-95.

Jones, M., Moore, M., & Snyder, R., (Eds.) Inside organizations, Sage, Thousand Oaks, 1988.

Karahanna, E., Straub, D., Chervany, N., 'Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs', MIS Quarterly, Vol. 23, No 2, 1999.

Kilmann, R., & Saxton, M., The Kilmann-Saxton culture gap survey. Organizational Design Consultants, Pittsburgh, 1983.

Koh, K., Ruighaver, A., Maynard, S., & Ahrnad, A, Security Governance: Its impact on Security Culture, 3rd Australian Information Security Management Conference, Perth, 2005.

Kruger, H., & Kearney, W., 'A prototype for assessing information security awareness'. Computers & Security, Vol. 25, No 4, 2006, pp. 289 – 296.

Lacey, D., Managing the Human Factor in Information Security: How to win over staff and influence business managers, Wiley, 2009a.

Lacey, D., 'Understanding and Transforming Organisational Culture', Proceedings of the Third International Symposium on Human Aspects of Information Security & Assurance, 2009b.

Leidner, D., & Kayworth, T., 'A review of culture in information systems research: towards a theory of information technology culture conflict', MIS Quarterly, Vol. 30, No 2, 2006, pp. 357-399.

Lim, J., Chang, S., Maynard, S., & Ahmad, A, Exploring the Relationship between Organizational Culture and Information Systems Security Culture, in Proceedings of the 7th Australian Information Security Management Conference, Edith Cowan University, 2009, pp. 87–97.

Malandrin, L., & Carvalho, T., 'Maintaining Information Security in the New Technological Scenario', Vol. 5, No 3, 2013.

Martins, A., & Eloff, J., Information Security Culture, 2002, p. 204-206.

Maynard, S., Exploring Organisational Security Culture – Research Model, 2002.

Maynard, S., & Ruighaver, A, Evaluating IS Security Policy Development, 2002.

McBride, M., Carter, L., & Warkentin, M., The Role of Situational Factors and Personality on Cybersecurity Policy Violation, Institute for Homeland Security Solutions, 2012.

McKinsey, Meeting the Cybersecurity Challenge, 2011.

Ministry of Finance of Finland, Effective Information Security, 2009.

Morris, M., Venkatesh, V., & Ackerman, P., 'Gender and age differences in employee decisions about new technology: An extension to the theory of planned behavior'. IEEE Transactions on Engineering Management, Vol. 52, No 1, 2005, pp. 69-84.

Ngo, L., IT Security Culture Transition Process, 2008.

Niekerk, J. Van., & Solms, R. Von., An holistic framework for the fostering of an information security sub-culture in organizations. Information Security South Africa (ISSA), 2005.

Nosworthy, J., Implementing information security in the 21st century - do you have the balancing factors?, 2000.

OECD, Digital Security Risk Management for Economic and Social prosperity, 2015.

O'Neill, B., Developing a Risk Communication Model to Encourage Community Safety from Natural Hazards, Fourth NSW Safe Communities Symposium, Sydney, 2004

Pahnila, S., Siponen, M., & Mahmood, A., Employees' behavior towards IS security policy compliance, Hawaii, 2007.

PCI Security Standards Council, Best Practices for Implementing a Security Awareness Program, 2014.

Peters, T., & Waterman, R., In search of excellence, HarperCollins, New York, 1982.

Ponemon Institute, The human factor in data protection [online], 2012.

Ponemon Institute, Cost of Cyber Crime Study and the Risk of Business Innovation, 2016.

Ponemon Institute, Cost of Data Breach Study, 2016.

Ponemon Institute, Cost of Data Breach Study, 2017.

Post, G., & Kagan, A., 'Evaluating information security trade-offs: restricting access can interfere with user tasks', Computers & Security, Vol. 26, No 3, 2007.

Ramachandran, S., Srinivasan, V., & Goles, T, 'Information Security Cultures of Four Professions: A Comparative Study'. Paper presented at the 41st Hawaii International Conference on System, Hawaii, 2004.

RAND, Cybersecurity economic issues, 2008.

Reid, R., & Van Niekerk, J., 'A Cyber Security Culture Fostering Campaign through the Lens of Active Audience Theory', HAISA, 2015, pp. 34-44.

Robbins, S., Organizational Behavior: Concepts, Controversies, and Applications (Fourth Edition ed.), Prentice Hall, New Jersey, 1989.

Roer, K., How to build and maintain security culture, 2014.

Roer, K., & Petrič, G., CLTRe Indepth insights into the human factor: The 2017 Security Culture Report, 2017.

Ross, S., & Masters, R., Creating a Culture of Security, 2011.

Rowe, D., Lunt, B., & Ekstron, J., The Role of Cyber-Security in Information Technology Education, 2011.

RSA, Translating Security Leadership into Board Value, 2017.

Sasse, A., 'Scaring and bullying people into security won't work', IEEE Security & Privacy, Vol. 3, 2015, pp, 80–83.

Sasse, A., & Smith, M., 'The Security-Usability Tradeoff Myth', IEEE Security & Privacy, Vol. 14, No 5, 2016, pp. 11-13.

Schein, E., Coming to a New Awareness of Organizational Culture, 1984, pp. 2-3.

Schein, E., Organizational Culture and Leadership, Jossey-Bass, San Francisco, 1992.

Schein, E., 'Empowerment, coercive persuasion and organizational learning: do they connect?', The Learning Organization, Vol. 6, No 4, 1999, pp. 163–172.

Schein, E., Organizational Culture and Leadership, 2004, p. 334.

Schlienger, T., Tool Supported Management of Information Security Culture, 2005.

Schlienger, T., & Teufel, S., Information Security Culture - the Social-Cultural Dimension in Information Security Management, 2002.

Siponen, M., & Willison, R., 'Information security management standards: Problems and solutions', Information & Management, Vol. 46, No 5, 2009, pp. 267-270.

Smircich, L., 'Concepts of culture and organizational analysis'. Administrative Science Quarterly, Vol. 28, 1983, pp. 339-358.

Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J., 'Analysis of end user security behaviors', Computers & Security, Vol. 24, No 2, 2005.

Susanto, H., Almunawar, M., & Tuan, Y., 'Information security management system standards: A comparative study of the big five', International Journal of Electrical Computer Sciences, Vol. 11, No 5, 2011, pp. 23-29.

Symantec, Internet Security Threat Report, 2017.

Tarimo, C., ICT Security Readiness Checklist for Developing Countries: A Social-Technical Approach, 2006.

Thomson, K., & von Solms, R., 'Information security obedience: a definition', Computer Security, Vol. 24, No 1, 2005, pp. 69–75.

Thomson, K., von Solms, R., & Louw, L., 'Cultivating an organizational information security culture', Computer Fraud Security, October, 2006, pp. 49–50.

Thompson, R., Higgins, C., Howell, J., 'Influence of experience on personal computer utilization', Journal of Management Information Systems, Vol. 11, No 1, 1994.

Trice, H., & Beyer, J., Using six organizational rites to change culture, Jossey-Bass, San Francisco, 1985, pp. 370–399.

Trice, H., & Beyer, J., The cultures of work organizations, Prentice Hall, Englewood Cliffs, 1993.

Van den Steen, E., On the Origin of Shared Beliefs (and Corporate Culture), MIT School of Management, 2005.

Van Niekerk, J., 'Establishing an information security culture in organizations: an outcomes based education approach', PhD diss., Nelson Mandela Metropolitan University, 2005.

Van Niekerk, J., A Holistic Framework for Fostering IS sub-culture in organizations: an outcomes based education approach, 2005.

Van Niekerk, J., & von Solms, R., An Holistic Framework for the Fostering of an Information Security Sub-Culture in Organizations, Centre for Information Security Studies, Nelson Mandela Metropolitan University, 2005.

Venkatesh, V., Morris, M., Davis, G., & Davis, F., 'User acceptance of information technology: toward a unified view', MIS Quarterly, Vol. 27, No 3, 2003.

Verizon, Data Breach Investigations Report, 2016.

Von Solms, B., 'Information Security -- the Third Wave?', Computers & Security, Vol. 19, No 7, 2000, pp. 615-620.

Von Solms, R., 'Information security management: why standards are important', Information Management & Computer Security, Vol. 7, No 1,1999, pp. 50-58.

Vroom, R., & von Solms, R., 'Towards information security behavioural compliance', Computer Security, vol. 23, no. 3, 2004, pp. 191–198.

Wasko, M., Faraj, S., 'It is what one does: why people participate and help others in electronic communities of practice', Journal of Strategic Information Systems, Vol. 9, 2000.

Weick, K., Sensemaking in organizations, Sage, Thousand Oaks, 1995.

World Economic Forum, A Framework for Assessing Cybersecurity Resilience, 2016.

Yanus, S., & Shin, R., Critical Success Factors for Managing an Information Security Awareness Programme, 2007.

Annex F: Questionnaires

Questionnaire for consultant/expert

BACKGROUND AND DEFINITION

Definition: *Cyber Security Culture (CSC) of organizations refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cyber security and how they manifest in people's behaviour with information technologies.*

1. Could you tell us what your role entails in relation to promoting cyber security culture as well as your background you have in cyber security??

2. The definition in the box above is the one adopted for this study. Would you change it in any way?

ORGANISATION'S CULTURE AND HOW CYBER SECURITY IS APPROACHED

3. What motivates companies to approach you (or other experts) to develop internal cyber security cultures?

4. How frequently should an organisations cyber security culture strategy/policy/training be updated? How should these updates be communicated?

5. In your experience is cyber security seen as primarily these people's responsibility within an organisation, or is it presented as something everybody needs to contribute to?
    a. Sole responsibility
    b. Collective contribution

6. In your experience, how involved is senior management in cyber security?

7. In your experience, how involved is middle management in the development and implementation of cyber security culture programmes?

8. What instruments would you recommend be used by organisations to promote CSC? [INDICATE ALL THAT APPLY]
    a. Posters
    b. Stories
    c. Flyers
    d. Tip sheets
    e. FAQ's
    f. Games
    g. Videos
    h. Presentations and input by external consultants
    i. Web resources
    j. Training

k. Certifications

ESTABLISHING A CYBER SECURITY CULTURE

9. To set up a CSC, or to bring about culture change, which **departments** within an organisation need to be involved and buy into this?

    a. Legal
    b. Risk/Compliance
    c. Finance
    d. IT department
    e. Security department
    f. Marketing / Communications department
    g. Human Resources department
    h. Other

10. Similarly, which **individuals** (C-Suite, department heads, staff) need to be involved and buy into this?

    a. Board of Directors
    b. CEO
    c. CFO
    d. CIO
    e. CSO/CISO
    f. Other senior management
    g. Vice Presidents
    h. IT Manager
    i. Security Manager
    j. Marketing / Communications Manager
    k. Human Resources Manager
    l. Other department directors / managers
    m. Staff in key partnering departments
    n. Other

11. Did you use a formal framework for setting-up/promoting/running your internal CSC? If 'yes' what was this / describe it.

12. Describe the steps involved in running a CSC programme (the table below provides a set of generic stages for the development and implementation of a CSC programme – we will use this to discuss how these steps match the actions in your organisation)

STAGE	ACTION	SPECIFIC QUESTIONS
Pre-treatment	Set up your core cyber security culture workgroup including representatives from core business teams, and board level sponsorship	Which departments and individuals need to be represented here?
Pre-treatment	Define main goals and target audience. Identify where security goals and activities conflict with other business processes in different departments	Is there usually sufficient communication and understanding between security teams and other business teams within an organisation?
Pre-treatment	Identify the current situation (s) and do a gap analysis to determine the difference between your current situation and your goal(s)	What metrics do you use to measure success for cyber security interventions?
Pre-treatment	Brainstorm a selection of activities to close the gap and create, develop or buy the necessary tools	In your experience, what activities have proven most successful in promoting cyber security awareness and culture change?
Treatment	Run activities	
Post-treatment	Rerun current situation metric and analyse the results to identify success levels	
Post-treatment	Review and consider your results. Consider what you would do differently. Revise accordingly	

13. How do you measure success of a CSC programme?
    a. What are the metrics you recommend be used?
    b. What metrics would you recommend be avoided?

14. If you were to produce a 'benchmark' of cyber security culture requirements for a company to judge itself against, which of the following would it contain and what would you add/subtract?

CYBER SECURITY IS:
1. Clearly communicated as an important organizational value
2. Treated as a risk to be mitigated and accounted for, rather than an expenditure
3. The responsibility of everyone in the organisation
4. A point of commitment and involvement of key departments, especially senior and middle management
5. Measured for its success. Objectives, milestones and processes are set and pursued.
6. Enforced through compliance mechanisms, e.g. sanctions and/or positive reinforcement mechanisms
Security practices (and training) are:
7. Tailored to the company's business and data
8. Tailored to the company's risk profile (who attacks them and why)

CYBER SECURITY IS:
9. Tailored to the employee's roles, functions and responsibilities
10. Are not too burdensome for employees considering their business responsibilities
11. Regularly updated (technology used is also updated)
12. Preventative rather than simply reactive
13. Ensured through sufficient resource and time allocation
Communication is:
14. Open and free flowing between and within departments
15. Through multiple communication channels, as appropriate
16. Personalised, impactful and tailored to content and recipients
17. Offering constant feedback to employees on their performance, their contribution to the company's cyber security, as well as applicable rewards and sanctions
18. Informing employees not only of secure practices, but also the variety of cyber threats

15. If I wanted to set up a cyber security culture in my own organisation and I came to you for advice, based on your experiences what things would you tell me that I absolutely must do to improve my chances for success?

16. What things would you tell me I absolutely must not do?

END OF INTERVIEW QUESTIONS

17. Do you want your name included in the final report?

18. Do you want your organisation acknowledged in the final report?

19. Is there anybody else you would recommend we interview?

Questionnaire for employee without CSC responsibilities

BACKGROUND AND DEFINITION

Definition: *Cyber Security Culture (CSC) of organizations refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cyber security and how they manifest in people's behaviour with information technologies.*

1. Could you tell us about your organisation and your role?

2. Have you ever heard of the term Cyber Security Culture? (if yes) What does the term mean to you – how would you define it? Have you ever heard CSC discussed in your organisation?

3. What responsibilities do you have, if any, in relation to promoting cyber security within your organisation?

YOUR ORGANISATION'S CULTURE AND HOW CYBER SECURITY IS APPROACHED

4. How is cyber security treated in your organisation?

5. Does your company have a cyber security strategy or policy?

6. Does your company provide you with cyber security training?
    a. If 'yes' describe this training and tell me what you thought of it

7. Is/Are the strategy/policy/training updated regularly?

8. How is that communicated to employees?

9. Do you perceive that the organisation as a whole is satisfied with the current state of cyber security rules and behaviour?

10. Who [which department] is in charge of cyber security within your organisation?

11. Who are you required to report cyber security incidents to?

12. Is cyber security seen as primarily these people's responsibility, or is it presented as something everybody needs to contribute to?

13. Are senior and middle management involved in cyber security?

14. Is there a clear commitment to cyber security and is that communicated openly to the organisation?

15. What are the instruments you use to promote CSC? [TICK ALL THAT APPLY]

    a. Posters
    b. Stories
    c. Flyers
    d. Tip sheets

e. FAQ's
f. Games
g. Videos
h. Presentations and input by external consultants
i. Web resources
j. Training
k. Certifications

COMPLIANCE WITH INTERNAL CYBER SECURITY RULES AND POLICIES

16. How is compliance with the rules secured?
    a. Are there sanctions in place?
    b. Are there positive reinforcement mechanisms, e.g. receiving more authority, positive feedback, rewards?
    c. Is there continuous feedback to employees?

17. How have cyber security rules impacted your job – both work-wise and time-wise?

18. How important do you believe cyber security rules are?

19. Do you believe other people in the organisation complies with cyber security rules?

20. Do you believe that your compliance makes a contribution to the cyber security of your organisation?

21. How easy is it for staff to notify security if they think they have done something that has created a cyber security threat, for example like clicking on a link in a suspect email message?
    a. Please describe the ways/means this is enabled

END OF INTERVIEW QUESTIONS

22. Do you want your name included in the final report?

23. Do you want your organisation acknowledged in the final report?

24. Is there anybody else in your organisation who we can interview? Also, do you have any contacts with people doing your role in other organisations that you could connect us to that might want to contribute to this study?

Questionnaire for employee with CSC responsibilities

BACKGROUND AND DEFINITION

Definition: *Cyber Security Culture (CSC) of organizations refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cyber security and how they manifest in people's behaviour with information technologies.*

1. Could you tell us about your organisation and your role?

2. Have you ever heard of the term Cyber Security Culture? (if yes) What does the term mean to you – how would you define it? Have you ever heard CSC discussed in your organisation?

3. What responsibilities do you have, if any, in relation to promoting cyber security within your organisation?

YOUR ORGANISATION'S CULTURE AND HOW CYBER SECURITY IS APPROACHED

4. Does your company have:
    a. a cyber security strategy
    b. a cybersecurity policy
    c. certification pursuant to a cybersecurity audit

5. Does your company offer cyber security training to:
    a. Staff
    b. Business partners
    c. Other stakeholders, e.g. customers

6. How frequently are your cyber security strategy/policy/training updated?

7. How is that (and its reasoning) communicated to employees?
    a. Newsletter
    b. Emails (by who?)
    c. Staff meetings
    d. Staff training and education
    e. Informal communication
    f. Other

8. Are you satisfied with the current state of cyber security rules and behaviour in your organisation?

    a. YES
    b. NO

9. Do you have a cybersecurity awareness-raising programme?
    a. YES
    b. NO

10. Do you have a cybersecurity staff education program?
    a. YES
    b. NO

11. Who [which department and /or role] is in charge of cyber security within your organisation? And who has operational responsibility?
    a. CEO
    b. CIO
    c. CSO
    d. CISO
    e. VP
    f. Director
    g. IT manager
    h. Other (specify)

12. Is cyber security seen as primarily these people's responsibility, or is it presented as something everybody needs to contribute to?

    a. Sole responsibility
    b. Collective contribution

13. Is senior management involved in cyber security?

14. Is middle management involved in the development and implementation of cyber security culture programmes?

15. What is CS budget as a percentage of IT budget and as a percentage of turnover

16. What are the instruments you use to promote CSC? [TICK ALL THAT APPLY]

    a. Posters
    b. Stories
    c. Flyers
    d. Tip sheets
    e. FAQ's
    f. Games
    g. Videos
    h. Presentations and input by external consultants
    i. Web resources
    j. Training
    k. Certifications

ESTABLISHING A CYBER SECURITY CULTURE

17. To set up a CSC, or to bring about culture change, which **departments** need to be involved and buy into this?

    a. Board of Directors
    b. Executive team
    c. Senior management
    d. CIO
    e. CSO

f. CISO
g. IT department
h. Security department
i. Marketing / Communications department
j. Human Resources department
k. Other

18. Similarly, which **individuals** (C-Suite, department heads, staff) need to be involved and buy into this?

a. CEO
b. CIO
c. CSO
d. CISO
e. Other senior management
f. Vice Presidents
g. IT Manager
h. Security Manager
i. Marketing / Communications Manager
j. Human Resources Manager
k. Other department directors / managers
l. Staff in key partnering departments
m. Other

19. Do you require certificates for specific roles and levels of responsibility in relation to cybersecurity? (If yes, which roles? What kind of certificates?)

20. Did you use a formal framework for setting-up/promoting/running your internal CSC? If 'yes' what was this / describe it.

21. Describe the steps involved in running a CSC programme (the table below provides a set of stages for the development and implementation of a CSC programme – we will use this to discuss how these steps match the actions in your organisation)

STAGE	ACTION	SPECIFIC QUESTIONS
Pre-treatment	Set up your core cyber security culture workgroup including representatives from core business teams, and board level sponsorship	Which departments and individuals need to be represented here?
Pre-treatment	Define main goals and target audience. Identify where security goals and activities conflict with other business processes in different departments	Is there usually sufficient communication and understanding between security teams and other business teams within an organisation?
Pre-treatment	Identify current situation (s) and do a gap analysis to determine the difference between your current situation and your goal(s)	What metrics do you use to measure success for cyber security interventions?

STAGE	ACTION	SPECIFIC QUESTIONS
Pre-treatment	Brainstorm a selection of activities to close the gap and create, develop or buy the necessary tools	In your experience, what activities have proven most successful in promoting cyber security awareness and culture change?
Treatment	Run activities	
Post-treatment	Rerun current situation metric and analyse the results to identify success levels	
Post-treatment	Review and consider your results. Consider what you would do differently. Revise accordingly	

22. How do you measure success of your programme? What are the metrics you use?
23. Do you subscribe to any (security management) standards?
24. Are you audited by a third party to ensure compliance?
25. If I wanted to set up a cyber security culture in my own organisation and I came to you for advice, based on your experiences what things would you tell me that I absolutely must do to improve my chances for success?
26. What things would you tell me I absolutely must not do?

Questionnaire for senior management

BACKGROUND AND DEFINITION

Definition: *Cyber Security Culture (CSC) of organizations refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cyber security and how they manifest in people's behaviour with information technologies.*

1. Can you tell us about your organisation and your current role, as well as any background you have in cyber security?
2. Have you ever heard of the term Cyber Security Culture? (if yes) What does the term mean to you – how would you define it? Have you ever heard CSC discussed in your organisation?
3. What responsibilities do you have, if any, in relation to promoting cyber security within your organisation?

YOUR ORGANISATION'S CULTURE AND HOW CYBER SECURITY IS APPROACHED

4. Does your company offer cyber security training to:
    a. Staff
    b. Business partners
    c. Other stakeholders e.g. customers

5. How frequently are your strategy/policy/training-documents updated? How are these updates communicated?

6. Are you satisfied with the current state of cybersecurity rules and behaviour in your organization?

    a. YES
    b. NO

7. Do you have a security awareness-raising program?
    a. YES
    b. NO

8. Do you have a staff education program?
    a. YES
    b. NO

9. Who [which department and /or role] is in charge of cyber security within your organisation? And who has operational responsibility?
    a. CEO
    b. CIO
    c. CISO
    d. VP
    e. Director
    f. IT manager
    g. Other (specify)

10. Is cyber security seen as primarily these people's responsibility, or is it presented as something everybody needs to contribute to?
    a. Sole responsibility
    b. Collective contribution

11. How is cybersecurity policy/policies communicated in the organisation?

12. Is there a CISO in the organisation?
    a. YES
    b. NO
    c. Reporting line to:

13. Is middle management involved in the development and implementation of cyber security culture programmes?

14. What is CS budget as a percentage of IT budget and as a percentage of turnover (optional)

15. What are the instruments you use to promote a CSC? [TICK ALL THAT APPLY]
    a. Posters
    b. Stories
    c. Flyers
    d. tip sheets
    e. FAQ's
    f. Games
    g. Videos
    h. Presentations and input by external consultants
    i. Web resources
    j. Training
    k. Certifications
    l. Other (please describe)

STRATEGIC ASPECTS OF CYBER SECURITY

16. Is cyber security an issue on your senior management agenda?

17. What instruments do you have in place?
    a. Strategy
    b. Policy
    c. Audits
    d. Certificates
    e. Other

18. Do you require your staff possess professional certifications for specific roles and levels of responsibility in relation to cybersecurity?
    a. (if yes) Does this extend to contractors and/or business partners?

19. Which certificates do you require?

20. What are the reasons for your involvement with cyber security – economic, legal, or other?

21. How do you measure success of your cyber security programme? What are the metrics you use?

COMPLIANCE WITH INTERNAL CYBER SECURITY RULES AND POLICIES

22. Are you, as senior management, trained in specific cyber security topics?

23. How is compliance with cybersecurity rules and policies ensured?
    a. Are there sanctions in place?
    b. Are there positive reinforcement mechanisms, e.g. receiving more authority, positive feedback, rewards?
    c. Is there continuous feedback?

24. How easy is it for staff to notify security if they think they have done something that has created a cyber security threat, for example like clicking on a link in a suspect email message?

a. Please describe the ways/means this is enabled

25. Is your organization compliant to any information/cyber security standards?
    a. YES (please name those relevant)
    b. NO

26. Are you audited by a third party to ensure compliance?

END OF INTERVIEW QUESTIONS

27. Have you had experience with a cyberattack? If yes what was the reaction of the staff? (optional)

28. In your view do you have a CSC in your organization?
    a. if not what can be done
    b. if yes what are the lessons learnt in all these years

29. Do you think a cyber security culture is important? Why?

30. Do you want your name included in the final report?

31. Do you want your organisation acknowledged in the final report?

32. Is there anybody else in your organisation who we can interview? Also, do you have any contacts with people doing your role in other organisations that you could connect us to that might want to contribute to this study?

ENIS

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-06-17-472-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-245-5
DOI: 10.2824/10543