REVIEW

Annals of Disaster Risk Sciences Vol 3, No 1 (2020): Special issue on cyber-security of critical infrastructure

Your Hospital Needs You: Eliciting Positive Cybersecurity Behaviours from Healthcare Staff

Dawn Branley-Bell, Northumbria University
Lynne Coventry, Northumbria University
Elizabeth Sillence, Northumbria University
Sabina Magalini, Fondazione Policlinico Universitario Gemelli
Pasquale Mari, Fondazione Policlinico Universitario Gemelli
Aimilia Magkanaraki, 7th Health Region of Crete
Kalliopi Anastasopoulou, 7th Health Region of Crete

Address for correspondence: Dr Dawn Branley-Bell, Psychology and Communication Technology Lab, Northumbria University, NB153, Newcastle upon Tyne, UK, e-mail: dawn.branley-bell@northumbria.ac.uk

Abstract

Staff behaviour plays a key role in the cybersecurity position of an organisation. Despite this, behaviour-change interventions are not commonly applied within the field of cybersecurity. Behaviour change technique could be particularly beneficial given increasing concerns around healthcare cybersecurity risks; particularly following the 2017 WannaCry ransomware attack which had devastating results on healthcare services. Cyber-risk is particularly concerning within healthcare given the criticality of medical systems and the potential impacts of a cyberbreach or attack. In worst case scenarios, cybersecurity incidents could result in patient harm or even fatalities. Whilst there has been concerted investment in improving healthcare's technological defences against cyberthreat, the same level of investment has not been made in healthcare staff. This has left staff behaviour as a vulnerability which can be exploited by attackers. This paper introduces a structured approach to help organisations work through four key steps that we refer to as the AIDE approach to Assess, Identify, Develop and Evaluate behaviour change techniques to facilitate more secure behaviour. We include a worked example of how we are applying this approach to the development of interventions to mitigate insecure cybersecurity behaviours in a healthcare context.

Keywords

Cybersecurity, Insecure behaviour, Healthcare, Security, Behaviour change

1. Introduction

Cybersecurity in healthcare (HC) traditionally lags behind other fields (Coventry & Branley, 2018) despite increasing concerns around cyberattacks and breaches (Albert, 2019). The WannaCry attack in 2017 is a widely recognised example of

the potential consequences of cyberattacks on the HC sector (Scott & Wingfield, 2017). WannaCry was a ransomware attack which affected over >100 countries. Within England, the attack resulted in the cancellation of over 19,000 patient appointments and a substantial financial cost to the National Health Service (National Audit Office, 2018). In addition to financial cost and loss of trust in the service, breaches have the potential to endanger human life (Kam, 2015).

Healthcare poses an attractive target for cybercrime due to the aforementioned weak security defences and the value of HC data (Coventry & Branley, 2018). On the black-market, HC data is currently more valuable than credit card details (Sulleyman, 2017). Healthcare also typically involves a wide network of interconnected devices, systems and databases.

Electronic sending of data between remote workers and other organisations provides even greater vulnerability (Coventry & Branley, 2018; Shenoy & Appel, 2017).

Staff behaviour has been identified as one of the major contributors to cybersecurity vulnerability (Hedström, Karlsson, & Kolkowska, 2013). However, it is important to recognise that staff – when acting securely - can also be one of the strongest protections against cyberthreat. Unfortunately, compared to investment in technological protection (e.g., firewalls, antivirus), investment in the human elements of cybersecurity pales in comparison (Coventry & Branley, 2018). Investment is generally restricted to awareness training, which on its own, does not facilitate behaviour change. Other interventions are required to provide staff with the tools and environment to act more securely. The improvement of HC security depends upon effective behaviour change (Michie, Atkins, & West, 2014).

The HC working environment has many characteristics that make behaviour change problematic. Staff are patient-focused, time-pressured, fatigued and stressed (Coventry et al., 2020; Coventry & Branley, 2018; Hall et al., 2017; Hall, Johnson, Watt, Tsipa, & O'Connor, 2016). Work culture can lead to security being overlooked or perceived as a burden, particularly if it is perceived to detract from patient care. The working environment is also prone to regular changes to team structure through rotation of staff members and new intakes of students. With this in mind, we suggest a holistic and dynamic methodological approach to behaviour change. The approach builds upon current theory and existing knowledge, whilst having the ability to evolve to reflect changes in the working environment.

1.1 Behaviour Change

There are many theories which identify factors underlying human behaviour, some of the most widely applied are the Theory of Planned Behaviour (TPB: Ajzen, 1985, 1991) which emphasises the role of attitudes, social norms and perceived control; The Integrated Behaviour Model (IBM: Fishbein, 2008) that expands upon the TPB by including knowledge and skills to perform the behaviour, salience of the behaviour, environmental constraints, and habit; and The Health Belief Model (Akey, Rintamaki, & Kane, 2013; Rosenstock, 1974, 1990) and Protection Motivation Theory (Rogers, 1975) that focus on perceived

threats and effectiveness of coping behaviour. These theories can guide the development of behaviour change interventions. Such interventions are made up of 'observable and replicable components' referred to as Behaviour Change Techniques (BCTs; Michie & Johnston, 2012). BCTs have been successfully applied across a range of domains including health (Turton, Bruidegom, Cardi, Hirsch, & Treasure, 2015) insurance adoption (van Winssen, van Kleef, & van de Ven, 2016) and promotion of environmentally green behaviours (Timlett & Williams, 2008). Despite success in other domains, BCTs have not been widely applied within cybersecurity (see Pfleeger & Caputo, 2012), and particularly not in the HC context. There is no single intervention that will work across all situations; effective change may require multiple levels and types of interventions. Many different BCTs exist – e.g., the Behaviour Change Technique Taxonomy project has identified 93 distinct BCTs (Michie et al., 2013). Due to this complexity, there have been many been numerous attempts to provide simpler frameworks to provide guidance. One widely applied approach is the MINDSPACE approach proposed by the UK's Institute of Government (Dolan, Hallsworth, Halpern, King, & Vlaev, 2010) which draws upon psychological theories, behavioural economics and 'nudge theory'. Nudging is the process of influencing decision making, and subsequent behaviour, by altering choice architecture or framing (Thaler & Sunstein, 2008). MINDSPACE consists of 9 components, these are summarised in Table 1.

Table 1. MINDSPACE (Dolan et al., 2010)

Component	Description
Messenger	We are heavily influenced by who communicates information to us. E.g., authority of the messenger can influence compliance or trust.
Incentives	We are often motivated by incentives (i.e., perceived rewards). We also tend to be influenced by predictable mental shortcuts (or 'heuristics') such as being loss-averse, i.e., having a strong instinct to avoid losses. Therefore framing incentives as loses rather than gains, can potentially have a stronger effect.
Norms	We are strongly influenced by what others do, or what we perceive them to do. Often we may not be aware that we are being influenced by others.
Defaults	We will often 'go with the flow' or pre-set or offered options, i.e., we will often stick with the default option if one is provided.
Salience	We are more likely to pay attention to something new, easy to understand and relevant to us.
Priming	Our behaviour can be influenced by sub-conscious cues.
Affect	Our emotions shape our decisions, therefore our emotional response to something can shape our actions.
Commitment	We seek to be consistent with our public promises, and reciprocate acts. E.g., if we have made a public commitment – such as an oral or written announcement - that we will do something, we are more likely to do so.
Ego	We prefer to act in ways that make us feel better about ourselves.

Frameworks such as MINDSPACE can help when co-designing interventions with end-users, as they provide a concise framework that does not require extensive exploration of the underlying theory; particularly beneficial when end-

extensive exploration of the underlying theory, particularly beneficial when end-user time is of limited resource, as is typical in HC. MINDSPACE was subsequently supplemented with EAST (Service et al., 2015) which explores more of the issues with implementation and evaluation of interventions and identifies that successful interventions need to be easy, social, attractive and timely.

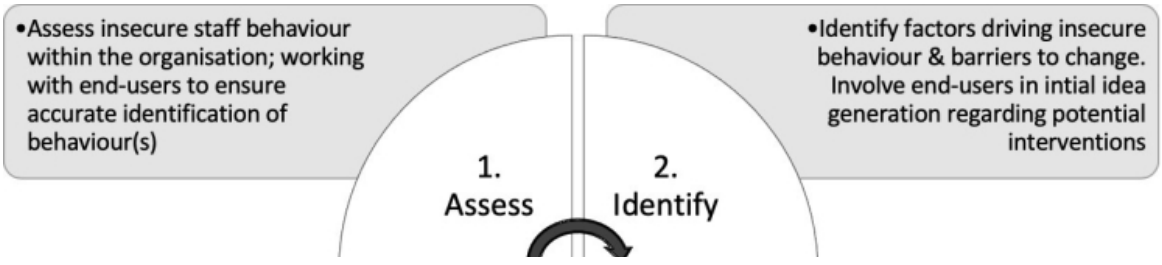
It is widely recognised in HC that behaviour change is not easy. One belief is that often interventions are too far removed from the context in which they will be implemented, and from potential barriers to successful implementation (Kelly & Barker, 2016). To address this, we will utilise Normalisation Process Theory (NPT; May & Finch, 2009) which identifies factors that promote and inhibit routine uptake of complex interventions into everyday HC practice. This is an action theory, concentrating on explaining what people *do*, rather than what they believe; and recognises the need to ensure that interventions need to be compatible with current clinical practice. NPT stresses the importance of distinguishing how the intervention differs from current processes, how end-users can collectively agree on the purpose of an intervention (and understand what is required of them) and their perceptions of the potential value of the intervention.

2. The AIDE approach

Although frameworks such as MINDSPACE provide a basis for developing interventions, they require that the researcher is at the stage where development can begin. However, there are two stages preceding this, firstly there is the need for effective – and accurate - identification of insecure behaviours in the workplace, and secondly there must be adequate identification of the factors driving the behaviours. Without this information, interventions may target the wrong behaviours or fail to address barriers.

Additionally, following the development of the intervention, there is a final stage that needs to be considered – evaluation and refinement.

One existing framework, SCENE (Coventry, Briggs, & Jeske, 2014), encompasses the MINDSPACE framework and addresses many of these issues, i.e., the need for co-creation of nudges, adequate identification of driving factors, and intervention evaluation. However, SCENE is specific to online nudges, it also does not take into account normalisation process for evaluation, nor the need to view this process as a reactive ongoing and evolving process. The AIDE approach expands upon this and provides a method to aid researchers - and importantly, HC organisations themselves - through four key stages for implementing effective behaviour change interventions (Fig. 1).



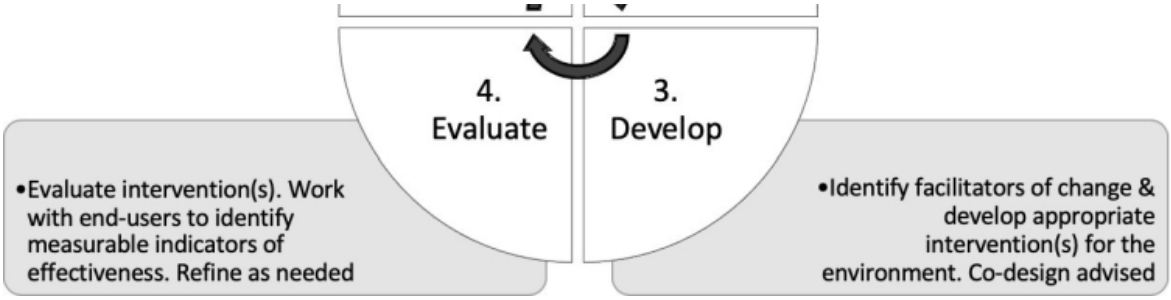


Figure 1. The AIDE Approach

This approach also provides the tools to regularly evaluate and refine the interventions to reflect changes in staff, team or organisational structure. This is important as security measures within HC need to be dynamic, realistic and time efficient. Relying upon a singular occurrence of BCT design is inadequate.

3. Piloting the approach

We are piloting this approach as part of a large EU project (Coventry et al., 2020; PANACEA Research). Here we will detail how we worked through each stage of the AIDE approach up to intervention development, and how we will evaluate and refine these interventions during the final stage of the project. Our research was approved by Northumbria University ethics committee.

3.1 Stage 1: Assess

The first stage involves identifying the type of insecure behaviour occurring within the working environment. It is not possible to design an effective intervention without identifying the key behaviours to target. To achieve this within our project, we conducted a set of workshops with staff across three different HC organisations, in three countries (Ireland, Italy and Greece). These workshops included a wide range of staff roles including medical administrators, IT staff, nurses, doctors, surgeons, residents and laboratory technicians. Staff involvement was strictly confidential.

Sessions were conducted face-to-face at the hospital location or remotely via Skype. Each session lasted between 45-60 minutes, and included between 2-9 staff members. A total of 50 staff took part across the three sites. For those interviewees that could not attend the focus groups (e.g., due to patient emergencies), we collected survey-based responses.

During the sessions, staff were asked to discuss the type of behaviour they see at work that may represent a cybersecurity weakness. The facilitators also asked other open-ended questions to prompt discussion, focusing on the following areas:

- Awareness of previous cybersecurity incidents at work
- Type of cybersecurity risks that staff felt were of most concern
- Type of data and technology that staff interact with on a daily basis and perceived security
- General awareness of potential cyber-risk and vulnerability to

By involving end-users we were able to identify a list of insecure behaviours to design interventions relevant to the sites in question. Workshop transcripts were analysed using thematic analysis, and we identified seven types of insecure behaviour: Poor computer and user account security; Unsafe e-mail use; Use of USBs and personal devices; Remote access and home working; Lack of encryption, backups and updates; Use of connected medical devices; and poor physical security. This stage of the research is reported in full in Coventry et al. (2020).

3.2. Stage 2: Identify

Having identified insecure behaviours occurring in the workplace, the second stage is to identify factors driving each behaviour. For example is this behaviour driven by a desire to prioritise speed of patient care? Or perhaps due to a lack of awareness? Without this information interventions are likely to be ineffective (Hedström et al., 2013).

Previous research has identified a range of factors that can drive insecure behaviour, such as perceived self-efficacy, security attitudes, external influences and threat evaluation (Blythe, 2013). It is also important to acknowledge that many insecure behaviours have been found to be instrumental, reasoned and conducted as a means to an end, e.g., to save time (Hedström et al., 2013).

To identify driving factors within our study, we conducted a second phase of workshops with HC staff across the three sites. Each workshop ran for a total of 3 hours. The sessions included between 15-25 staff members per group, a total of 56 staff took part across the three HC sites. Again, staff included the same wide range of roles to ensure that we gained a wide perspective. This time staff were presented with two priority behaviours. These behaviours were chosen by senior staff members at each location (from the seven behaviours identified in the first phase), according to those that they felt were most relevant/concerning for their particular working environment. As HC staff time is limited, this enabled us to explore the most critical security priorities in more depth.

The workshops began with the facilitators providing a short overview from the first workshop. Staff were then provided with information on the behaviours they would be discussing and informed that the goal of the workshop was to identify why these behaviours may be occurring. Staff were split into small groups of 3-5 members and provided with worksheets to help start discussion. The worksheets (Appendix A) were based upon common factors identified by behavioural theories and accompanying crib sheets were provided (Appendix B). The crib sheets were translated into the local language of each site to aid staff members who were not fluent English speakers. Following the group work, everyone was brought back together to for a final overall discussion and summary of key findings.

Thematic analysis of the workshop transcripts identified several facilitators of insecure behaviour: lack of cybersecurity awareness, time pressure and fatigue, behaviour prioritisation (i.e., staff priority is patient care and cybersecurity can be seen as a barrier or burden), mutual trust amongst colleagues, lack of reinforcement, and insecure behaviours necessary to complete their job

(Coventry et al., 2020).

We encouraged staff to feel free to share any suggestions they may have regarding how things could be improved. However, it is interesting to note that staff generally felt disempowered to change things – largely due to feeling that the insecure behaviour was necessary to do their job. E.g., staff found it difficult to identify interventions to prevent use of USB devices, as no alternative method was available. Consequently, the only intervention they suggested was a technological intervention, e.g., using password-protected, encrypted USB devices. Likewise, staff only identified one potential intervention for encouraging secure sending of patient information, which was a technological intervention to automatically detect if confidential documents are being attached to an e-mail to prevent sending. This highlights how, in some situations, technological changes may be more appropriate than behavioural interventions.

3.3. Stage 3: Develop

The third stage of the AIDE approach consists of intervention development. Insecure behaviour and facilitating factors have been identified in the preceding two stages, therefore the researchers can start to identify appropriate interventions. It is likely that this third phase will provide numerous intervention options, and not all may be feasible, appropriate or necessary. Examples of the potential interventions identified in our own study are shown in Table 2. We also identified a range of environmental changes which could be used to facilitate secure behaviour. E.g., introducing an improved login process to reduce burden on staff due to effort and time spent logging in/out, or changing the policy so that passwords no longer have to be changed so often (unless password is compromised).

Table 2. Example of interventions identified during PANACEA research

Intervention Type	Examples
Messenger	• Messages from patients about protecting their lives and keeping their data private
Incentives	• Have a regular award within the company for appropriate behaviour and/or display a message thanking staff for using the approved, secure process • Loss framing nudge (*disincentive*): Alert users that insecure behaviour could result in loss of their personal files/work/salary information • Pop up message every X mins if the user engages in an insecure behaviour (*disincentive*)
Norms	• Poster campaign showing senior staff acting securely and/or supporting secure behaviour
Defaults	• Enable auto-log out, disable ‘remember me’ option, disable USB port; autoscan USB.

Salience & Priming	• "Just because something hasn't happened yet, doesn't mean it won't. Don't get complacent! XX% of HC organisations, like this one, have been affected by some form of cyberattack or data breach" (also related to *Norms*). • Risk level: Provide an indication of risk level, this could use visual aids such as a traffic light system displaying red for high risk, green for low risk. E.g., in relation to password security or the level of attacks IT is defending • "Technology alone cannot prevent all cyberattacks/cyber risk. Ensure you are taking responsibility for your own safety" – and bite- sized tips on how to achieve
Affect	• Highlight potential negative impact on patients if breach/attach occurs.
Commitment	• Display all actions conducted on the staff members computer account that day & require approval by asking the staff member to tick a box to say they have reviewed all of these actions and confirm they conducted or approved these
Ego	• Display a message thanking staff for acting securely and therefore helping to ensure patient safety and data privacy.

The next step that we recommend is the development of a set of criteria to enable the researchers and end-users to collaboratively identify the final interventions for prototype development. The criteria we used in our study is presented in Table 3, with each item scored on a scale of 1-5. Criteria may differ according to context.

Table 3. Criteria for identification of final interventions for prototype development

Criterion	Description
Technological feasibility	The feasibility of implementing any hardware or software required for the intervention. This must take into account the technology already in use and how feasible it would be to introduce the necessary components.
Time and ease of implement [R]	Time and ease of implementing the complete intervention, this includes design, piloting, integration of any technological components, staff training, intervention materials etc.
Disruption to work processes [R]	Any disruption to other work process that could occur as a result of introducing the intervention. E.g., reduced staff time due to training needs,
Requires policy change [R]	Whether the intervention requires a change to company and/or governmental policy.
Financial cost [R]	The degree to which implementing (and running) the intervention is financially costly for the organisation.

Estimated effectiveness'	Estimated effectiveness based upon existing literature or previous experience relating to this behaviour change approach.
Sustainability	Long-term sustainability of the intervention within the organisation.
Generalisability	Whether the intervention is only suitable for a specific, niche context or whether it has the potential to be applied in a wider context.

Note: R = Reverse scored

Using the criteria, a team of researchers should independently score each identified nudge. Once completed, the scores should be tested for interrater reliability using Cohen's kappa (for 2 raters) or Fleiss' kappa (for 3+ raters). Reliability should be >0.80 – a commonly accepted level of strong agreement. If reliability is <0.80, it is recommended that the researchers meet to discuss the scores causing the discrepancies and work towards mutual agreement. If agreement is not forthcoming, the criteria may not be well defined and may require amendment until adequate interrater reliability is achieved.

The overall scores can then be used to narrow down the potential interventions to the final choices (i.e., those scoring most highly). It is recommended that the selected interventions are then presented to end-users to sense check and help identify potential barriers to implementation and/or adoption. Final choices for prototype development will be chosen based upon this end-user feedback. Prototypes should also be co-designed with end-users, using a feedback loop to refine the prototype, and initial pilot sessions using a representative group of end-users.

3.4. Stage 4: Evaluate

Once prototypes have been refined and are ready for the implementation, they will be evaluated within the working environment. To achieve this, researchers and end-users must work together to explicitly identify measurable outcomes that can be used as success metrics (or validation indicators). Whenever possible, these metrics should include an objective technological measure and a baseline measure for comparison, e.g., phishing penetration test results before and after an anti-phishing intervention is introduced. It is also beneficial to supplement empirical, technological results with self-reported feedback from the end-users (e.g., via interview or survey). This enables the researchers to gain more insight into why and how the intervention may be being successful (or not) and may also highlight potential revisions to improve effectiveness. In some instances, technological measures may be difficult to obtain and more reliance may be necessary upon self-reported measures.

It is important to note that success metrics will differ significantly depending upon the environment and targeted behaviour(s) – which further supports the application of customisable approaches such as the AIDE approach. Once metrics have been identified and measured, this completes the first iteration of the AIDE approach. However, this is designed to be an ongoing, reiterative and dynamic process (Fig. 1) that evolves with the working environment. This is particularly important as the HC environment changes regularly including new staff intake, staff rotation, introduction of new devices, system updates etc.

Without this dynamic approach, interventions may fail to reflect the current cybersecurity position and priorities. The AIDE approach should be regularly used to re-assess and re- evaluate current behaviour and interventions.

4. Conclusion

To summarise, the AIDE approach introduces a novel framework to structure and guide the application of behaviour change interventions within the working environment, including within HC. Rather than focusing upon how to develop a particular intervention (as methodologies already exist for this, e.g., MINDSPACE: Dolan et al., 2010), this approach provides a framework to structure the entire process from the initial stages of assessing problematic behaviours and identifying underlying motivations, through to developing an appropriate intervention (including evaluating suitability and effectiveness), and onto continued reassessment. Although we have demonstrated this approach in relation to the HC environment – its dynamic process means that it is easily generalised across many settings.

The AIDE approach encompasses the importance of involving end-users in the process of behaviour change development. It is possible that with adequate training and support, this approach could also be used to build a toolkit to enable end-users, such as HC organisations, to apply this process 'in-house'. This is something that the PANACEA project aims to deliver.

5. References

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. In *Action Control*. https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Akey, J. E., Rintamaki, L. S., & Kane, T. L. (2013). Health Belief Model deterrents of social support seeking among people coping with eating disorders. *Journal of Affective Disorders*, *145*(2), 246–252.

Albert, M. (2019). "Why do we need to wait for people to be hurt?" Medical cyber attacks soar 1400%. Retrieved October 11, 2019, from https://www.sfgate.com/healthredesign/article/medical-cyber-attacks-terrorism-hospital-health-13853912.php

Blythe, J. M. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. In *Proceedings of CHI 2013 Doctoral Consortium*. Retrieved from http://chitaly2013.disi.unitn.it/wp-content/uploads/2013/08/CHItaly_DC_Blythe.pdf

Coventry, L., Branley-Bell, D., Magalini, S., Mari, P., Magkanaraki, A., & Kalliopi, A. (2020). Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. In *Lecture Notes in Computer Science*.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative

review of trends, threats and ways forward. *Maturitas*, *113*, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Coventry, L., Briggs, P., & Jeske, D. (2014). SCENE: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment. https://doi.org/10.1007/978-3-319-07668-3_23

Dolan, P., Hallsworth, M., Halpern, D., King, D., & Vlaev, I. (2010). *MINDSPACE:Influencing behaviour through public policy*. Retrieved from https://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf

Fishbein, M. (2008). A Reasoned Action Approach to Health Promotion. *Medical Decision Making*, *28*(6), 834–844. https://doi.org/10.1177/0272989X08326092

Hall, L. H., Johnson, J., Heyhoe, J., Watt, I., Anderson, K., & O'Connor, D. B. (2017).Exploring the Impact of Primary Care Physician Burnout and Well-Being on Patient Care. *Journal of Patient Safety*, 1. https://doi.org/10.1097/PTS.0000000000000438

Hall, L. H., Johnson, J., Watt, I., Tsipa, A., & O'Connor, D. B. (2016). Healthcare Staff Wellbeing, Burnout, and Patient Safety: A Systematic Review. *PLOS ONE*, *11*(7), e0159015. https://doi.org/10.1371/journal.pone.0159015

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals the importance of user rationale.*Information Management and Computer Security*. https://doi.org/10.1108/IMCS-08- 2012-0043

Kam, R. (2015). The human risk factor of a healthcare data breach - Community Blog. Retrieved April 10, 2018, from https://searchhealthit.techtarget.com/healthitexchange/CommunityBlog/the-human-risk- factor-of-a-healthcare-data-breach/

Kelly, M. P., & Barker, M. (2016). Why is changing health-related behaviour so difficult?*Public Health*, *136*, 109–116. https://doi.org/10.1016/j.puhe.2016.03.030

May, C., & Finch, T. (2009). Implementing, Embedding, and Integrating Practices: An Outline of Normalization Process Theory. *Sociology*, *43*(3), 535–554. https://doi.org/10.1177/0038038509103208

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

Michie, S., & Johnston, M. (2012, March). Theories and techniques of behaviour change: Developing a cumulative science of behaviour change. *Health Psychology Review*. https://doi.org/10.1080/17437199.2012.654964

Michie, S., Richardson, M., Johnston, M., Abraham, C., Francis, J., Hardeman, W., … Wood, E. (2013). The behavior change technique taxonomy (v1) of 93 hierarchically clustered techniques: Building an international consensus for the reporting of behavior change interventions. *Annals of Behavioral Medicine*, *46*(1), 81–95. https://doi.org/10.1007/s12160-013-9486-6

National Audit Office. (2018). *Investigation: WannaCry cyber attack and the*

National Audit Office. (2018). *Investigation: WannaCry cyber attack and the NHS*. Retrieved from https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS-Summary.pdf

PANACEA Research. (2020). Retrieved January 27, 2020, from https://panacearesearch.eu/ Pfleeger, S. L., & Caputo, D. D. (2012). *Leveraging Behavioral Science to Mitigate Cyber Security Risk*. Retrieved from https://ai2-s2- pdfs.s3.amazonaws.com/e755/aa8baf01ef655ef7b1472ceba505b7c45b91.pdf

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*. https://doi.org/10.1080/00223980.1975.9915803

Rosenstock, I. M. (1974). The Health Belief Model and Preventive Health Behavior. *Health Educ Behav*, *2*(4), 354–386. https://doi.org/10.1177/109019817400200405

Rosenstock, I. M. (1990). The Health Belief Model: Explaining Health Behavior Through Expectancies. *Health Behavior and Health Education: Theory, Research, and Practice*.

Scott, M., & Wingfield, N. (2017, May 13). Hacking attack has security experts scrambling to contain fallout. *The New York Times*. Retrieved from https://www.nytimes.com/2017/05/13/world/asia/cyberattacks-online-security-.html

Service, O., Hallsworth, M., Halpern, D., Algate, F., Gallagher, R., Nguyen, S., … Kirkman, (2015). *EAST Four simple ways to apply behavioural insights*.

Shenoy, A., & Appel, J. M. (2017). Safeguarding confidentiality in electronic health records. *Cambridge Quarterly of Healthcare Ethics*, *26*(2), 337–341. https://doi.org/10.1017/S0963180116000931

Sulleyman, A. (2017, February 12). NHS cyber attack: Why stolen medical information is so much more valuable than financial data | The Independent. *The Independent*. Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and hapiness. Focus*.

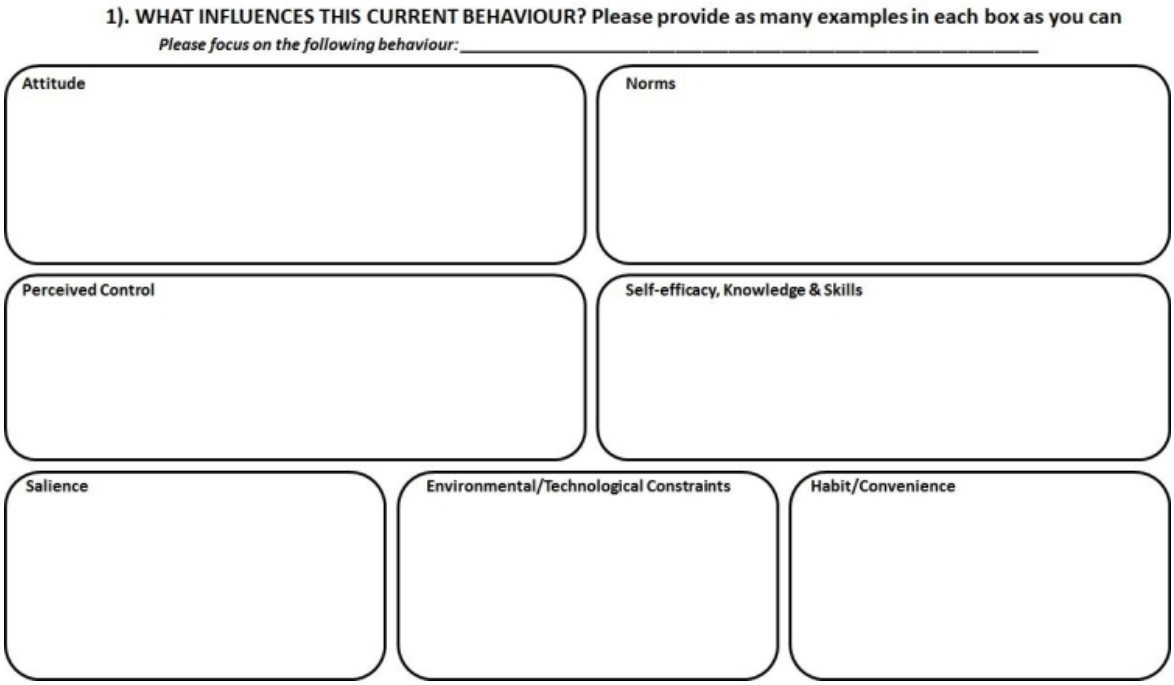
Timlett, R. E., & Williams, I. D. (2008). Public participation and recycling performance in England: A comparison of tools for behaviour change. *Resources, Conservation and Recycling*, *52*(4), 622–634. https://doi.org/10.1016/j.resconrec.2007.08.003

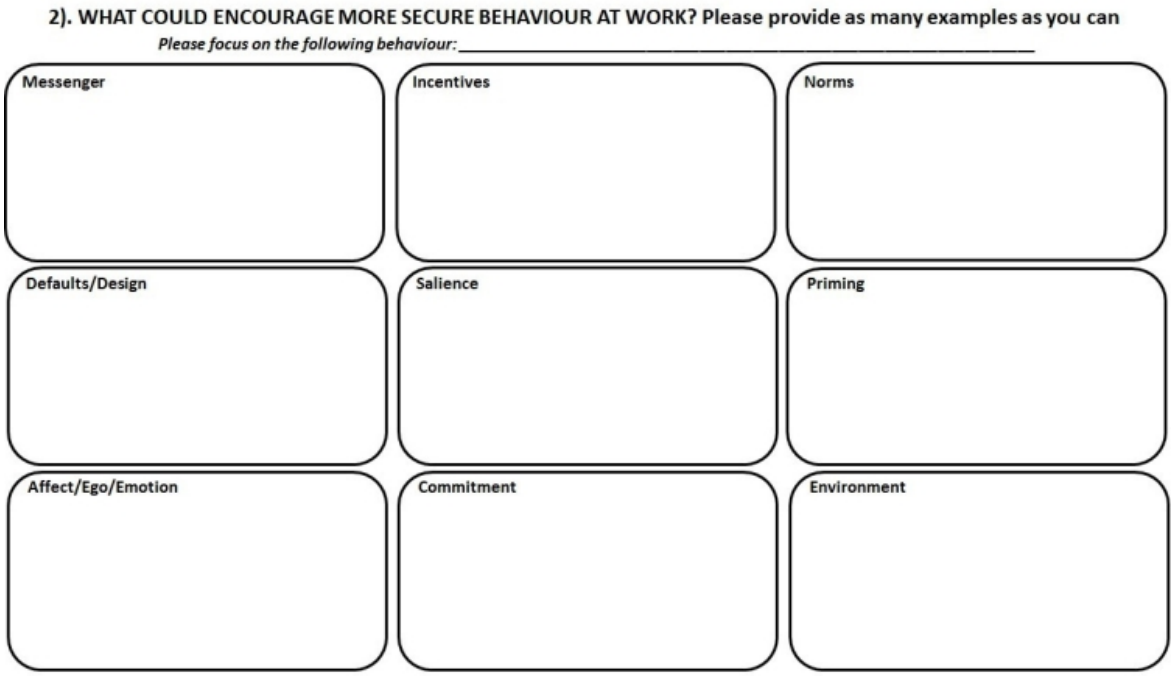
Turton, R., Bruidegom, K., Cardi, V., Hirsch, C. R., & Treasure, J. (2015). Novel methods to help develop healthier eating habits for eating and weight disorders: A systematic review and meta-analysis. *Neuroscience and Biobehavioral Reviews*, *61*, 132–155. https://doi.org/10.1016/j.neubiorev.2015.12.008

van Winssen, K. P. M., van Kleef, R. C., & van de Ven, W. P. M. M. (2016).

Potential determinants of deductible uptake in health insurance: How to increase uptake in The Netherlands? *The European Journal of Health Economics*, *17*(9), 1059–1072. https://doi.org/10.1007/s10198-015-0745-2

6. Appendix A: End-user Workshop Worksheets





7. Appendix B: End-user Workshop Crib Sheets

Current Behaviour (Worksheet 1)

ATTITUDE:

- **Experiential Attitude –** How do you feel about the identified risky behaviour? And how do you feel about acting more securely – do you generally feel positively or negatively and why?

Do you think acting securely at work is beneficial or a hindrance? Do you have mixed feelings about this behaviour – if so, can you explain why? How do you think your feelings affect your behaviour?

- **Instrumental attitude -** What are the costs and benefits of behaving more securely, in relation to this risky behaviour? Are the benefits generally greater than the costs?

Can you think of any benefits of behaving more securely – for example, do you get rewarded for this behaviour at work? Would acting more securely help or hinder your day to day work?

NORMS:

- **Injunctive Norm -** Do your work colleagues ever give you the impression that they think *you* should carry out this behaviour?

For example, do they ever expect you – or ask you - to conduct this behaviour?

- **Descriptive Norm –** How do your work colleagues behave at work?

Do you see your work colleagues conducting the identified risky behaviour at work?

PERCEIVED CONTROL:

- How much control do you feel you have over this risky behaviour (and acting more securely) in the workplace?

Do you feel it is within your control to act in a more secure manner, or do you think there is anything stopping you from doing so?

SELF-EFFICACY, KNOWLEDGE & SKILLS:

- Are you confident about your ability to behave in a more secure manner? Alternatively, if you are not confident, does this drive the identified risky behaviour?
- What knowledge and skills do you think are needed to enable you to be able to behave more securely, in relation to the identified risky behaviour?

What training do you currently receive? Do you think this is sufficient? If not, how would you improve upon this? Is there anything else outside formal training, that you feel has (or could) provided you with the knowledge and skills to behave more securely?

SALIENCE:

- What prompts or reminds you to behave securely at work (in relation to the identified behaviour)? *For example, are there any relevant posters to raise awareness? Alerts on the workstations or by e- mail?*

ENVIRONMENTAL AND/OR TECHNOLOGICAL

CONSTRAINTS:

- In what ways does your environment create barriers to secure behaviours? In what way does your environment and/or the technology you use encourage the identified risky behaviour?

This could include your working environment, daily responsibilities and/or the computer systems.

HABIT AND/OR CONVENIENCE:

- Do you think the identified risky behaviour has become habitual at work?

For example, do you feel this behaviour is part of the normal working culture amongst yourself, or other staff members? Or do you think people engage in this behaviour for convenience?

Behaviour Change (Worksheet 2)

MESSENGER: Who do you think would be the most effective person(s) to communicate security information at work, in relation to this behaviour? Who would people listen to or not listen to? Who would people believe?

Are you more likely to listen to information/advice about this behaviour from your manager or your peers? What about governmental advice?

INCENTIVES: What incentives (or sanctions) might encourage secure behaviour, and/or discourage the identified risky behaviour?

Do you think rewards (e.g., verbal praise, bonuses, or another form of positive recognition) would be effective in encouraging secure behaviour? Do you think punishments (e.g., fines, warnings, or other forms of negative recognition) would be effective in discouraging unsecure behaviour. Which do you think would work best?

NORMS: How could norms be influenced to encourage more secure behaviour (and/or discourage the identified risky behaviour)? Whose security behaviour influences other peoples' security behaviour?

How do you think changing the social norms in the workplace (e.g., how colleagues are behaving, or how colleagues expect others to behave) could influence this behaviour in others? Can you think of any ways to do this? Who do you think would influence others' behaviour more (e.g., peers, senior staff, IT staff etc)?

DEFAULTS/DESIGN: Where could defaults be used to encourage secure behaviour and develop secure habits?

What defaults do you think should be offered on workstations to encourage more secure behaviour and/or discourage the identified risky behaviour? What other design changes can you think of to encourage more secure behaviour?

SALIENCE: What things could be introduced to increase your awareness of risk in relation to this behaviour? What would make people feel that cybersecurity is an important issue?

Would posters in the workplace help at all? How about alerts via e-mail or on the computer screens? What else do you think could help

raise your awareness of the risk related to this behaviour?

PRIMING: What might be used to prime or prompt more secure behaviour? What can be used to keep security in peoples mind?

Can you think of any targeted prompts or security-related questions or alerts that could help while you are using the workstations? E.g., would it be helpful to have a reminder about cyberrisk when you log on, or when you perform certain tasks related to this behaviour? Do you think visual indicators of safety would be helpful?

AFFECT/EGO/EMOTION: Is there any way to use emotion to encourage more secure behaviour (and/or discourage the identified risky behaviour)? What would make people feel positive or negative about security behaviours?

Do you think asking staff to reflect upon how they feel about security (or how they would feel if they were the victim of a cyberattack) would be helpful at all?

How could security be encouraged as something that people feel is important to them and their self- image? What would make people feel confident in their security behaviours?

What could encourage staff to feel pride in their secure behaviour? For example, would some kind of award/recognition system be effective? Can you think of any other suggestions?

COMMITMENT: What kind of commitment/agreement to act securely, might be helpful?

Would signing a written agreement to behave according to security guidelines encourage you to act more securely? Can you think of any other steps that staff could take to indicate – and/or encourage - their commitment to acting securely?

ENVIRONMENT: In what ways could your environment be changed to encourage more secure behaviours and/or discourage the identified risky behaviour?

Is there anything about your working environment, daily responsibilities and/or the computer systems at work, which could be changed to make it easier to behave securely (or conversely more difficult to behave insecurely)?

Copyright (c) 20212021 Annals of Disaster Risk Sciences

This work is licensed under a Creative Commons Attribution 4.0 International License.