Promoting Cybersecurity Culture Change in Healthcare

Healthcare Cybersecurity Culture

Dawn Branley-Bell
Northumbria University, Newcastle upon Tyne, England, UK. dawn.branley-bell@northumbria.ac.uk

Lynne Coventry
Northumbria University, Newcastle upon Tyne, England, UK. lynne.coventry@northumbria.ac.uk

Elizabeth Sillence
Northumbria University, Newcastle upon Tyne, England, UK. elizabeth.sillence@northumbria.ac.uk

Cybersecurity problems have traditionally been addressed through technological solutions and staff training. Whilst technology can reduce or remove some weaknesses some attacks specifically target human users. Whilst training can educate staff on *how* to behave more securely, this is often not sufficient to promote actual secure behaviours . Knowing what to do is necessary but not sufficient. It is also necessary to remove barriers to the required behaviour and to intervene in a way that affords behaviour change. This is particularly true in healthcare, where environmental factors including time pressure, and staff fatigue can create barriers for cybersecurity behaviour change. Technology and training are only a partial solution. Only by taking a more holistic approach which encompasses technology, people and processes and addressing the culture change needed to facilitate more secure behaviours will any progress be made in the workplace. We conducted a series of in-depth interviews and workshops with staff across 3 healthcare organisations in Italy, Crete and Ireland. This

paper reflects on our main findings, including key requirements for future cybersecurity interventions. We used this reflection to develop a secure behaviour toolkit to help healthcare organisations identify problematic behaviours, co-create interventions to increase secure staff behaviour being mindful that sometimes culture change is necessary to enable the required security behaviours. The toolkit also provides a means to evaluate the interventions identified and the final implementation of the intervention.

CCS CONCEPTS • Security and Privacy • Human and society aspects of security and privacy • Social aspects of security and privacy • Usability in security and privacy

Additional Keywords and Phrases: cybersecurity, healthcare, culture, behaviour change, toolkit

1 Introduction

Cybersecurity has traditionally been approached by technological solutions, staff training and awareness raising. It is now generally acknowledged that technology alone is not sufficient to prevent cyberattacks and breaches [8,16]. Staff must be willing and able to enact the required behaviours. There may be organisational barriers to this enactment, the removal of which will require cultural change and/or behaviour change. In this introductory section we recap on healthcare's vulnerability to cyber risk, why we need to move to a more holistic approach to cybersecurity and our rationale for building a set of tools to help healthcare organisations (HCOs) address these issues.

1.1 Healthcare and cyber risk

Good cybersecurity is essential to protect an organisation from both informational or data breaches and cyberattacks, and to enable organisations to incorporate technology effectively into their workplace in a safe and positive manner. This is particularly important in healthcare where cyberattacks could involve not only disclosure of sensitive patient data but cyberattacks could disrupt a HCO's ability to provide patient care, by reducing the availability and/or accuracy of medical devices which creates a detrimental impact on patient wellbeing and ultimately even result in deaths. In a holistic sense cybersecurity ensures that data, the infrastructure, and individual medical devices are secure.

One of the most widely recognised cyberbreaches in healthcare is the 2017 WannaCry ransomware attack. WannaCry targeted computers running the Microsoft Windows NT operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. Although the attack was not specifically aimed at healthcare, it significantly impacted on the UK's National Health Service (NHS) which was brought to a standstill [15]. There have been significant increases in the prevalence and severity of cyberattacks on hospitals and health systems during 2020 and healthcare has been described as the primary target for cybercrime [6]. In November 2020, the US Federal Government announced that ransomware attacks on healthcare organisations was "credible, ongoing and persistent" [3]. The UK has also seen continued increases in cyberattacks on HCOs, particularly in 2020 – driven partly by attackers using the COVID-19 pandemic as another avenue to exploit [25].

Healthcare is an attractive target for cybercrime for two fundamental reasons: it is a rich source of valuable data (patient data is now worth more than credit card details on the dark net [19]) and its cybersecurity defenses tend to be weak [4]. Increasing amounts of interconnected devices, and electronic sending of data between remote workers and other organisations increases vulnerability [4,18]. In addition to this, staff often experience fatigue which can lead to human error [4,5,9,10].

There are severe and widespread implications of an HCO cyberbreach, including impacts on staff and patient wellbeing and financial costs. For example, the aforementioned WannaCry attack on the NHS resulted affected at least 80 out of the 236 trusts across England and 603 primary care and other NHS organisations (including 595 GP practices) [15]. The

attack caused staff to be locked out of HCO devices, preventing - or at least significantly delaying - access to, and updating of, patient information, sending of test results to GPs or other HCOs, use of medical equipment and devices (e.g., radiology and pathology), and testing of medical samples. As a consequence, it is estimated that more than 19,000 appointments were cancelled, operations were postponed, and many patients had to travel further to A&E departments [15]. Cancellations included urgent cancer appointments, causing worry and distress for patients [13]. In addition to negative impacts on patient wellbeing, there were also huge financial impacts, including an economic loss of £5.9 million due to lost patient admissions, lost A&E activity and cancelled outpatient appointments [7]. The true cost of the attack is not known as other costs were accrued for example, additional IT support cost of restoring data and systems, and NHS staff overtime [15]. It is estimated that the total cost of the attack for the NHS may be around £92 million [23].

1.2 The need for culture change

The operability of HCOs has never been more vulnerable to cybersecurity attacks. Recent security reports suggest that employee noncompliance with organisational cybersecurity policies may be partly to blame (e.g., [31]). Staff behaviour has been shown to be one of the major contributors to cybersecurity vulnerability [8,11], with some studies suggesting that human error accounts for up to 95% of breaches [16]. Insecure behaviour by an employee can render even the most sophisticated defensive technologies useless. Attackers are well aware of this, and rather than spending hours trying to break through the technological defenses, they are targeting users to let them in [29]. Unfortunately, current perspectives on cybersecurity have been found to be too narrow, with a tendency to overlook human factors; instead focusing upon technological solutions [8,16,28]. Whilst humans have often been described as cybersecurity's 'weakest link' [11]. It is important to recognise that staff can also be one of the strongest links in cybersecurity, when secure employee behaviour acts – in effect – as a 'human firewall' [2,32]. Unfortunately, work culture can mean that security is not recognised as a priority or is perceived as a burden -particularly if it is perceived to detract from patient care [2,5]. Security researchers suggest that workplace culture needs to incorporate cybersecurity to change attitudes towards good security behaviours [1,24]. A strong cybersecurity culture can help to reduce the likelihood of noncompliance with the security policy and thus minimize the threat resulting from human behaviour. However, this should not only focus on behaviour change but also ensuring that the behaviours required are accepted, understood and achievable within the organisation.

Increasing training can address knowledge and skills but there is a substantial body of research that indicates that whilst knowledge and awareness is necessary, this alone is not necessarily enough to translate into actual behaviour [2,14] and affect cultural change Many other factors including attitudes, norms, personal agency, salience and habit can also influence staff behaviour [4,8]. Alshaikh [1] suggests that organisations need to exceed the minimal requirement of ensuing that staff have regular awareness training; instead, substantial investment is required to enable a transformative change that develops a cybersecure work culture. We need to bridge the gap between knowledge and action. Bridging the gap requires understanding both the barriers to such a culture and what is required to remove those barriers. In addition, we need to understand motivators within the specific organisation and how these can be applied to change both attitudes and behaviours. An ideal security culture was identified by De Veiga et al. [24] not only as being an aware and knowledgeable workforce but one whose behaviours are conscientious and care about complying with the security policies.

Some research has explored the factors that influence cybersecurity culture in organizations. Da Veiga et al.'s [24] review paper identifies a number of factors that affect cybersecurity culture. These include external environmental and internal organisational factors. External factors include political, legal factors and technological factors; while internal factors include organisational factors, management factors including policy, human factors, and trust. An ideal organisation is seen as one that is proactive and facilitates open engagement with its employees around the issues and actions that would affect the organisation.

To affect such change and create a more open and engaged workforce around cybersecurity, we suggest adopting a holistic, systematic, and co-creative approach to cybersecurity. This includes moving towards culture change and changing staff mindset; for example, getting all stakeholders on board and refocusing their thinking away from cybersecurity simply for compliance and towards seeing it as an issue of patient protection and privacy. This need for culture change led to our development of a toolkit for HCOs, to help them to build a good cybersecurity culture and promote positive behaviour change in the workplace.

2 Method

To guide our development of the toolkit, we conducted a series of workshops with healthcare staff from HCOs across three countries (Italy, Crete, and Ireland). These workshops were designed to provide further insight into the HCO working environment, staff experiences, attitudes and behaviours, and to explore potential barriers and facilitators to secure behaviour. For the purposes of the toolkit development, we sought to understand the key requirements of a more holistic approach to cybersecurity within HCOs. Each workshop took place as a 3-hour session with approximately 15-25 staff members taking part (with the exception of one occasion when due to logistic reasons and staff availability, the session was split into three 1-hour sessions, with approximately 5-10 staff taking part in each session). The workshops included a range of roles and levels including doctors, nurses, administration staff, IT staff, residents/students and other HC professionals. During the workshops, staff were asked to discuss experiences of insecure behaviours in the workplace [5] and explore the facilitators of these behaviours, and conversely, barriers to secure behaviour. The sessions were anonymous and confidential, and care was taken to structure the groups so that participants would as comfortable as possible having an open discussion (e.g., avoiding the inclusion of line managers in the same group as their direct reportees and including IT staff as a separate group).

3 Results

Reflecting on our discussions with HCO staff, it is apparent that culture change and a more holistic approach to cybersecurity is required. In particular, organisational acceptance of poor behaviour, onboarding processes and existing access controls were identified as barriers to more secure behaviours [5]. In this section we reflect on key requirements for developing an approach to build a stronger cybersecurity culture and future cybersecurity interventions.

3.1 Requirement 1: Insight driven, patient focused and non-burdensome

Prior to developing any intervention(s), it is important to develop an understanding of the key characteristics of the target staff team(s). This includes identifying their roles and responsibilities, the team hierarchy, current security culture and attitudes and the type of computer equipment and other technological devices they have access to. When identifying group roles, it's important to recognise that shadow working processes may be present. Shadow working refers to individuals conducting daily tasks and activities that are outside of their written job description; this was something we found to be common within HCOs. We found that time pressures often resulted in senior staff delegating tasks to junior/admin staff, to enable them to prioritise patient care. These tasks could include making appointments, entering notes onto the system and in some cases even issuing prescriptions:

> "Surgeons could not do surgery if they spent all their time making appointments"
> "We have to go around it [the system], to do our work"

Some junior staff explained that they are often overlooked and do not receive security training (or are last in line to do so), even though they hold sensitive information, such as senior staff's passwords:

> "Admin get forgotten about, despite having everyone's password! We are not considered important for security"

Therefore, when investigating staff roles and responsibilities, it is important not to rely solely upon 'official' written job descriptions. Without this knowledge, targeted interventions may miss key staff members.

It is also vital to accurately capture staff priorities; within healthcare this is often focused on patient care. Knowledge of staff priorities and motivations will help you to identify drivers of insecure behaviour. HCO staff are often overworked, fatigues and under extreme time pressure [4,5,9,10]. We found that many 'unofficial workarounds' were used by staff as they were perceived as quicker, easier and therefore less of a barrier to treating their patients. Security can be perceived as a burden if it is thought to create a barrier to staffs key priorities. For these reasons, cybersecurity interventions must be as brief and non-burdensome as possible.

"It is not possible to remember 20 different passwords"
"Logging in on their own account would be a positive thing to do, but it is time consuming"

Take time to identify what staff truly value in the workplace, and where their priorities lie; this can help you to make cybersecurity more salient and relevant to them. For instance, if focusing on patient care is driving staff to act insecurely (for example, using unofficial workarounds with the aim of speeding up patient treatment), then it may be more effective to reframe the information provided to them to emphasis how insecure behaviour could impact negatively upon the patient. Figure 1 shows some examples of posters framed in this manner.

Figure 1. Examples of cybersecurity posters framed around patient risk

3.2 Requirement 2: Timely and relevant

It is widely recognised in healthcare 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 [12]. For this reason, cybersecurity interventions must be personal and relevant, not generalised. It is not effective to bombard staff with *all* cybersecurity information, *all* the time. They will simply stop paying attention. This also applies if they are presented with information that is completely irrelevant to their current situation! Different issues will be important and/or salient at different times, therefore information must be context specific and timely. Timeliness is particularly important for interventions based on behavioural nudging, as nudging works by promoting the desired behaviour at the point of behavioural decision making. Interventions must relate to vulnerabilities in the users' current environment and encourage behaviours that are realistic and achievable.

3.3 Requirement 3: Pro-active and achievable

Fear is often not enough to change behaviour. Campaigns and nudges based upon fear appeals tend to result in individuals ignoring the information altogether. Effectively, as the fear is too great, individuals stop paying attention to the message (sometimes referred to as 'burying one's head in the sand'). In other instances, individuals can also react by denying the threat, again as a way to deal with the associated fear [17]. In other circumstances, individuals may simply get resilient to the fear, as reflected on by one of our interviewees:

> "I've worked here for 40 years, nothing is going to scare me, I've seen it all"

To be effective, it is important to provide employees with information on how to practically - and achievably - reduce risk. This is often referred to as 'coping information' and it can provide staff with a sense perceived control over the situation. Coping information must be simple enough to be followed so that the individual feels confident that they can realistically achieve the recommended behaviour. This feeds into the individuals perceived control and self-efficacy. If the suggested coping behaviour sounds too complex, it is less likely that the employee will perceive it as achievable or 'worth it'.

Another aspect of achievability, beyond self-efficacy, is whether the encouraged behaviour is realistic for the individual's responsibilities. For example, some HCO staff reflected on being discouraged to click on e-mail attachments or weblinks, despite needing to do this as part of their daily responsibilities:

> "We could not do our daily work without being able to open attachments or links. Also, internal hospital admin emails include clickable links and attachments!"

3.4 Requirement 4: Reiterative and dynamic

The healthcare environment is always changing, for example there are regular intakes of new staff, staff rotations, introduction of new medical devices and system updates. It is imperative that any approach to encouraging secure behaviour can evolve with the working environment. Interventions must be routinely and regularly evaluated on an ongoing, reiterative basis. Without this dynamic approach, interventions may fail to reflect the current cybersecurity position and priorities. For example, some of the staff in our workshops reflected on new staff experiencing delays in receiving their own logins for the computer systems – therefore staff felt unable to follow security protocols as they were forced to share their logins with new staff during this period. Similarly, staff reflected on not wanting to install the latest computer updates and patches, as every time they do "it breaks something, and we have to get IT to fix it". In much the same way, guidance and training must be up-to-date and reflect any new software, technology, and processes within the workplace.

4 Secure Behaviour Toolkit

The findings from our work across the HCOs have fed into the development of a toolkit that captures the requirements across three key stages. Requirement 1 is captured in stage 1 "Identifying and understanding risks and insecure behaviour" Requirements 2 & 3 are captured in the second stage "Encouraging positive behaviour change" and Requirement 4 is captured in the third stage "Evaluation and Reassessment". The three stages are then broken down into six easy-to-follow tools, to help HCOs iteratively identify and address cybersecurity issues, with an emphasis upon promoting positive behaviour change, i.e., more secure behaviour (Figure 2).

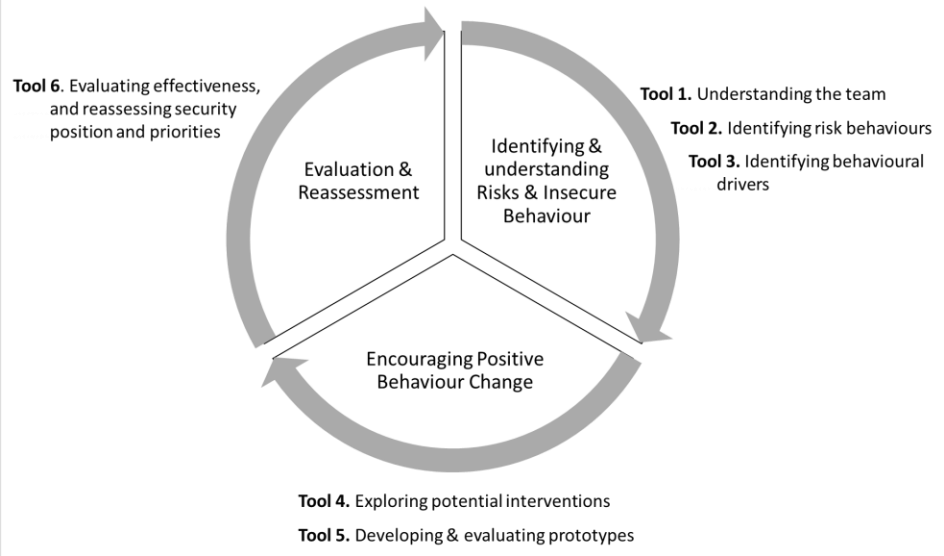

Figure 2. Secure Behaviour Toolkit Overview

The toolkit is aimed at staff responsible for encouraging cybersecure behaviours within the HCO and is designed to provide effective but easy to administer methods. The user is not required to be a technical or cybersecurity expert. Cybersecurity can be perceived as difficult and technologically complex, however with the right tools it is possible to make good cybersecurity decisions without needing to know all the technical details, which is the rationale for the toolkit.

The toolkit encompasses a behavioural nudging approach. Behavioural nudges are small changes to the environment or choice architecture that encourage an individual to make a particular choice or behave in a particular way. They rely largely upon triggering automatic cognitive processes and biases. Behavioural nudges have been shown to be effective in many different contexts (e.g., promoting positive health behaviours [22,30], insurance adoption [26,27], and promotion of environmentally green behaviours [20]). Nudging has not been as widely applied within cybersecurity; however, research suggests that nudging can also be effective in this area [21]. The toolkit aims to apply this approach to promote security in healthcare.

In keeping with the aim of promoting a holistic approach to cybersecurity, the toolkit also signposts to other interventions where appropriate, including training, technological solutions, and changes to policy. As aforementioned, often a combination of approaches is likely to be the most effective. Take for example, the use of USB devices - this could be tackled in many ways. Behavioural nudges can be used to encourage more secure use (by raising awareness of risk, nudging staff to scan before use and use only for work, encourage password protection and encryption etc.). However, should the organisation wish to ban the use of such devices, a technological intervention could be much more effective such as deactivating all USB ports. Or if some USB use is essential, using a combination of technological and behavioural interventions by deactivating unnecessary USB ports and using behavioural nudges to encourage secure usage when required. The decision of whether to apply behaviour nudges, technological interventions, policy changes or a combination, is one that must be decided by the HCO in question, taking into account their unique working environment, the behaviours concerned, and legal, moral, and professional responsibilities. The toolkit is designed to help them work through these decisions. Another critical component of the toolkit is its focus on cybersecurity as an

ongoing process. The tools are designed to be applied on a reiterative basis, allowing the organisation to reassess and update its security approach to suit the changing work environment.

5 Conclusion

Human factors of cybersecurity continue to be overlooked, despite technological solutions being insufficient to address all cyber risk. It is important that the importance of human factors is recognised at the organisational and board level. However, it is also vital that security culture within the workplace is also addressed. This is particularly true in healthcare, where environmental factors including increased connectivity of medical devices, time pressure, focus on patient care and staff fatigue further increase cybersecurity vulnerability. A more holistic approach to cybersecurity must be promoted. To this aim, we developed a secure behaviour toolkit to help healthcare organisations promote secure staff behaviour. The process identified four key requirements for future cybersecurity interventions within healthcare. Interventions must be *insight-driven, patient focused and non-burdensome; timely and relevant; pro-active and achievable;* and *reiterative and dynamic.* The secure behaviour toolkit can provide the user with accessible tools to help satisfy these requirements within their HCO.

ACKNOWLEDGMENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826293.

REFERENCES

<bib id="bib1"><number>[1]</number> Moneer Alshaikh. 2020. Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security* 98, (November 2020), 102003. DOI:https://doi.org/10.1016/j.cose.2020.102003 </bib>
<bib id="bib2"><number>[2]</number> Dawn Branley-Bell, Lynne Coventry, Elizabeth Sillence, Sabina Magalini, Pasquale Mari, Aimilia Magkanaraki, and Anastasopoulou Kalliopi. 2020. Your hospital needs you: Eliciting positive cybersecurity behaviours from healthcare staff using the AIDE approach. *Annals of Disaster Risk Sciences* (2020). </bib>
<bib id="bib3"><number>[3]</number> CISA. 2020. *Ransomware Activity Targeting the Healthcare and Public Health Sector*. Retrieved February 11, 2021 from https://us-cert.cisa.gov/ncas/alerts/aa20-302a </bib>
<bib id="bib4"><number>[4]</number> Lynne Coventry and Dawn Branley. 2018. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas* 113, (2018), 48–52. DOI:https://doi.org/10.1016/j.maturitas.2018.04.008 </bib>

<bib id="bib5"><number>[5]</number> Lynne Coventry, Dawn Branley-Bell, Elizabeth Sillence, Sabina Magalini, Pasquale Mari, Aimilia Magkanaraki, and Kalliopi Anastasopoulou. 2020. Cyber-Risk in Healthcare: Exploring Facilitators and Barriers to Secure Behaviour. In *Lecture Notes in Computer Science*, A Moallem (ed.). Springer, Cham, 105–122. DOI:https://doi.org/10.1007/978-3-030-50309-3_8 </bib>
<bib id="bib6"><number>[6]</number> Laura Dydra. 2020. The 5 most significant cyberattacks in healthcare for 2020. *Becker's Health IT*. Retrieved February 11, 2021 from https://www.beckershospitalreview.com/cybersecurity/the-5-most-significant-cyberattacks-in-healthcare-for-2020.html </bib>
<bib id="bib7"><number>[7]</number> S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi, and P. Aylin. 2019. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digital Medicine* 2, 1 (October 2019), 1–7. DOI:https://doi.org/10.1038/s41746-019-0161-6 </bib>
<bib id="bib8"><number>[8]</number> Henry Glaspie and Waldemar Karwowski. 2018. *Human Factors in Information Security Culture: A Literature Review*. DOI:https://doi.org/10.1007/978-3-319-60585-2_25 </bib>
<bib id="bib9"><number>[9]</number> Louise H. Hall, Judith Johnson, Jane Heyhoe, Ian Watt, Kevin Anderson, and Daryl B. O'Connor. 2017. Exploring the Impact of Primary Care Physician Burnout and Well-Being on Patient Care. *Journal of Patient Safety* (November 2017), 1–1. DOI:https://doi.org/10.1097/PTS.0000000000000438 </bib>
<bib id="bib10"><number>[10]</number> Louise H. Hall, Judith Johnson, Ian Watt, Anastasia Tsipa, and Daryl B. O'Connor. 2016. Healthcare Staff Wellbeing, Burnout, and Patient Safety: A Systematic Review. *PLOS ONE* 11, 7 (July 2016), e0159015–e0159015. DOI:https://doi.org/10.1371/journal.pone.0159015 </bib>
<bib id="bib11"><number>[11]</number> Karin Hedström, Fredrik Karlsson, and Ella Kolkowska. 2013. Social action theory for understanding information security non-compliance in hospitals the importance of user rationale. *Information Management and Computer Security* (2013). DOI:https://doi.org/10.1108/IMCS-08-2012-0043 </bib>
<bib id="bib12"><number>[12]</number> Michael P. Kelly and Mary Barker. 2016. Why is changing health-related behaviour so difficult? *Public Health* 136, (July 2016), 109–116. DOI:https://doi.org/10.1016/j.puhe.2016.03.030 </bib>
<bib id="bib13"><number>[13]</number> Sarah Marsh. 2017. NHS cancer patients hit by treatment delays after cyber-attack. *The Guardian*. Retrieved February 11, 2021 from http://www.theguardian.com/society/2017/may/14/nhs-cancer-patients-treatment-delays-cyber-attack </bib>
<bib id="bib14"><number>[14]</number> Susan Michie, Lou Atkins, and Robert West. 2014. *The Behaviour Change Wheel: A Guide to Designing Interventions*. Silverback Publishing, London, UK. </bib>
<bib id="bib15"><number>[15]</number> 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 </bib>
<bib id="bib16"><number>[16]</number> Calvin Nobles. 2018. Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration* 9, 3 (December 2018), 71–88. DOI:https://doi.org/10.2478/hjbpa-2018-0024 </bib>
<bib id="bib17"><number>[17]</number> Robert A C Ruiter, Loes T E Kessels, Gjalt-Jorn Y Peters, and Gerjo Kok. 2014. Sixty years of fear appeal research: current state of the evidence. *International journal of psychology : Journal international de psychologie* 49, 2 (April 2014), 63–70. DOI:https://doi.org/10.1002/ijop.12042 </bib>
<bib id="bib18"><number>[18]</number> Akhil Shenoy and Jacob M. Appel. 2017. Safeguarding confidentiality in electronic health records. *Cambridge Quarterly of Healthcare Ethics* 26, 2 (2017), 337–341. DOI:https://doi.org/10.1017/S0963180116000931 </bib>
<bib id="bib19"><number>[19]</number> Aatif Sulleyman. 2017. 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 </bib>
<bib id="bib20"><number>[20]</number> R. E. Timlett and I. D. Williams. 2008. Public participation and recycling performance in England: A comparison of tools for behaviour change. *Resources, Conservation and Recycling* 52, 4 (February 2008), 622–634. DOI:https://doi.org/10.1016/j.resconrec.2007.08.003 </bib>
<bib id="bib21"><number>[21]</number> James Turland, Lynne Coventry, Debora Jeske, Pam Briggs, and Aad van Moorsel. 2015. Nudging towards security. In *Proceedings of the 2015 British HCI Conference on - British HCI '15*, ACM Press, New York, New York, USA, 193–201. DOI:https://doi.org/10.1145/2783446.2783588 </bib>
<bib id="bib22"><number>[22]</number> Robert Turton, Kiki Bruidegom, Valentina Cardi, Colette R Hirsch, and Janet Treasure. 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, (December 2015), 132–155. DOI:https://doi.org/10.1016/j.neubiorev.2015.12.008 </bib>
<bib id="bib23"><number>[23]</number> UK Department of Health and Social Care. 2018. *Securing cyber resilience in health and care*. Retrieved February 11, 2021 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf </bib>
<bib id="bib24"><number>[24]</number> Adéle da Veiga, Liudmila V. Astakhova, Adéle Botha, and Marlien Herselman. 2020. Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security* 92, (May 2020), 101713. DOI:https://doi.org/10.1016/j.cose.2020.101713 </bib>
<bib id="bib25"><number>[25]</number> Helen Warrell. 2020. More than one in four UK cyber attacks related to Covid-19. *Financial Times*. Retrieved February 11, 2021 from https://www.ft.com/content/f3d638f1-ff3c-4f8c-9a78-b96eec9c2cb8 </bib>
<bib id="bib26"><number>[26]</number> K. P. M. van Winssen, R. C. van Kleef, and W. P. M. M. van de Ven. 2016. Potential determinants of deductible uptake in health insurance: How to increase uptake in The Netherlands? *The European Journal of Health Economics* 17, 9 (December 2016), 1059–1072. DOI:https://doi.org/10.1007/s10198-015-0745-2 </bib>
<bib id="bib27"><number>[27]</number> W J Wouter Botzen, Joop De Boer, and Teun Terpstra. 2013. Framing of risk and preferences for annual and multi-year flood insurance q. (2013). DOI:https://doi.org/10.1016/j.joep.2013.05.007 </bib>
<bib id="bib28"><number>[28]</number> Heather Young, Tony van Vliet, Josine van de Ven, Steven Jol, and Carlijn Broekman. 2018. Understanding Human Factors in Cyber Security as a Dynamic System. In *Advances in Human Factors in Cybersecurity* (Advances in Intelligent Systems and Computing), Springer International Publishing, Cham, 244–254. DOI:https://doi.org/10.1007/978-3-319-60585-2_23 </bib>
<bib id="bib29"><number>[29]</number> Xichen Zhang and Ali A. Ghorbani. 2020. Human Factors in Cybersecurity: Issues and Challenges in Big Data. *Security, Privacy, and Forensics Issues in Big Data*, 66–96. DOI:https://doi.org/10.4018/978-1-5225-9742-1.ch003 </bib>

<bib id="bib30"><number>[30]</number> Ying Zhang and Richard Cooke. 2012. Using a combined motivational and volitional intervention to promote exercise and healthy dietary behaviour among undergraduates. *Diabetes Research and Clinical Practice* 95, 2 (2012), 215–223. DOI:https://doi.org/10.1016/j.diabres.2011.10.006 </bib>
<bib id="bib31"><number>[31]</number> 2019. *Global Threat Intelligence Report*. NTT Security. Retrieved March 9, 2021 from https://www.nttsecurity.com/docs/librariesprovider3/resources/2019-gtir/2019_gtir_report_2019_uea_v2.pdf </bib>
<bib id="bib32"><number>[32]</number> Building Organizational Risk Culture in Cyber Security: The Role of Human Factors | SpringerLink. Retrieved February 23, 2021 from https://link.springer.com/chapter/10.1007/978-3-319-94782-2_19 </bib>