Good practices for cybersecurity behaviour change interventions

Letting users experiment, witness the repercussions of their behaviours and improve accordingly is highly effective in information security interventions. Hence researchers should consider decision making as an essential feature of further studies in the domain. Interventions should also be adapted to the target audience, as we saw that for example senior citizens may not be able to learn at the same pace as youngsters (Blackwood-Brown et al., 2019). Slower, time-spaced trainings could prove to be a better fit depending on the circumstances.

Successful interventions aimed at businesses should not come in a single shot but rather in the form of repeated training (Da Veiga, 2015) or even be a definite party of the work environment (Busch et al., 2015). Employees should be given the chance to express themselves and exchange with their colleagues, in order to learn from one another rather than from a single vertical authority (Albrechtsen and Hovden, 2010). Researchers should also consider engaging and entertaining interventions so that target users feel more comfortable with the topic (Busch et al., 2015; He et al., 2019).

Introduction

Cyber security should be an integral part of people's decision-making processes when building and operating a business, as well as in individual usage of products and services. In more recent years, the UK government has increased efforts in securing organisations and their digital presence. The DCMS has therefore been investing and investigating the factors that drive a strong investment in cyber security solutions and raising awareness of the consequences. We have taken the step towards this direction by exploring the human factors and educational solutions that have been implemented to tackle these issues.

Policy context

Digital technologies are essential tools of our modern society. With this, cyber threats have exploded in numbers and variety, from individual credit card fraud to massive breaches of private data (e.g. Playstation Network, Equifax). Consequently, there is an urgent need for cybersecurity solutions. IT workers can come with technical means to strengthen computing infrastructures; however, attackers are always ready to exploit the system using human vulnerability. This

weakness can be addressed by raising awareness and breeding good practices for everyone. We performed a systematic literature review of all studies related to the effectiveness of online behaviour change interventions. After filtering, a very low number of 13 relevant items were eventually found. We were able to gather from these, evidence of good and bad practices. However, it is clear, that there is a lack of research in the domain.

This review focuses on how effective various "behaviour change interventions" in cybersecurity are altering the short-term as well as long-term behaviour of persons in a variety of populations or contexts. It aims to inform policymakers as well as businesses seeking to provide their employees with the most effective forms of behaviour change intervention.

The question we focus on is the following.

How effective are cybersecurity behaviour change interventions in improving security behaviours amongst businesses and individuals?

Businesses

Learning from each other is an effective route for employees to improve. Albrechtsen and Hovden (2010)[1] found that a good strategy is to let the security officials presenting the workshop take a backseat approach and let the employees do all the talking and thinking together. This can pool their knowledge and allow them to learn from one another easily. As a result, the workshop intervention significantly changed both awareness– i.e., attitudes and knowledge about information security – and self-perceived behaviour. The effect either remains stable or increases over time, the six-month-later survey indicates. The study also showed that getting the employees to discuss their ideas of solutions or approaches to scenarios in front of security officials is a good way for the security officials to gain knowledge of how employees work, how they approach cybersecurity issues, and where some key "social" vulnerabilities might exist in the company. Thus, this sort of workshop also boasts that double-edged benefit of unveiling some potential shortcomings in the company's organisation in addition to raising awareness amongst employees.

Interventions should be tailored to each company and its stakeholders, rather than offer the same generic model for all. Da Veiga (2015)[2] suggests to specifically calibrate them to the target

[1] E. Albrechtsen and J. Hovden. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4):432, June 2010. ISSN 01674048.

[2] A. Da Veiga. An information security training and awareness approach (ISTAAP) to instil an information security-positive culture. In Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), pages 95–107, 2015.

company, and further refine for each category of employees. Lasting positive effects were demonstrated, as scores on the ISCA survey[3] significantly increased over the years. Mohammed and Apeh(2016)[4] propose a similar method for school staffs and show promising short-term results. Da Veiga (2015) also found that the whole endeavour could be thwarted by internal restructuration of the company, thus requiring a recalibration of the information security training in these cases. This shows that the method is fragile and sensitive to changes in the organisation.

Interventions should be repeated over time. Mohammed and Apeh (2016), show significant increase in the appropriate handling of malicious emails one-month after a training on the topic but do not assess long-term effect. Same goes for Hagen and Albrechtsen (2009)[5], who document significant post-experiment general improvements in security knowledge, awareness, and behaviour for employees trained with an e-learning tool. Despite positive immediate results, authors warn about the lack of long-term assessment, claiming that short-term individual improvements do not necessarily make for global organisational learning. The whole is greater than the sum of its part, an important point to consider when designing intervention models. This issue is addressed by Da Veiga (2015) who shows promising results with interventions that were repeated each year in the target company.

Effectiveness of a continuous model implemented in the everyday work life through a workstation-integrated app. Busch et al. (2015)[6] prove that this could overcome problems inherent to yearly interventions mentioned above. The rationale behind it is two-fold, keeping the training constant and increasing the employees' motivation to comply with the policies in place. No more intermittent, sporadic interventions. Here employees are directly involved in a constant, background information security awareness policy through a workstation-integrated app.

Positive results were observed with various real-time features such as communication of risks associated with employees' actions, statistics about general security compliance and small individual challenges (e.g., "Comply with all security policies for one week.") whose completion was rewarded with points. Competition between users (e.g., "Behave more securely than your colleagues for one week") could also be a factor of improvement **but at the risk of harming the company's social culture**. Authors also argue that these kinds of games are more attractive than formal, dry information security classes. It makes learning more enjoyable and rewarding, which helps employees understand that cybersecurity is not some obscure high-tech feature reserved for computer scientists but something that everyone should care about.

---

[3] A. Veiga and N. Martins. Information security culture and information protection culture: A validated assessment instrument. Computer Law & Security Review, 31, 04 2015. doi: 10.1016/j.clsr.2015.01.005.

[4] S. Mohammed and E. Apeh. A model for social engineering awareness program for schools. In 2016 10th International Conference on Software, Knowledge, Information Management Applications (SKIMA), pages 392–397, 2016.

[5] J. Hagen and E. Albrechtsen. Effects on employees' information security abilities by e- learning. Information Management and Computer Security, 17(5):388–407, 2009. doi: 10.1108/09685220911006687.

[6] M. Busch, S. Patil, G. Regal, C. Hochleitner, P. Fröhlich, and M. Tscheligi. A behavior change support system to help employees protect organizational information security. 2015.

Individuals

Personal responsibility is key in improving information security. Witnessing the consequences of their actions made people more aware of the information security risks and let them adjust their behaviour accordingly. Shillair et al. (2015)[7] for example, built a training model relying on this and based on vicarious experience. Zhou et al. (2018)[8] conducted a study where participants had to choose security settings in a simulated health data application, witness the impact of their choices on the security of their private data, and then could review the parameters. Between 21-32% of the participants chose stronger security settings after witnessing the effect on their private data. This reflects the previously discussed work of Busch et al. (2015), who showed that communicating employees the risks associated with their behaviour was key in improving information security. Personal responsibility was also a key feature in the intervention proposed by Shillair et al. (2015).

Hence, when people are shown the potential impact of their actions, **it is likely that they will adjust their behaviour in consequence**. Giving users freedom to try and see seems to be an essential feature of information security intervention. Abd Rahim et al. (2019)[9] corroborate this statement as they evaluate a government cybersecurity awareness program aimed at youth aged 12-19 in schools. The findings were consistent with the theory that youngsters require guidance in their Internet usage as they were found to be lacking in self-regulation. They also lacked judgement especially in differentiating between legitimate and illegitimate applications available over the web. The researchers found that by adding a decision-making process as part of the cybersecurity awareness message, the youth could get better insights about sharing their private data online.

Effectiveness of individual-aimed interventions might vary depending on the target population. Shillair et al. (2015) remark that training should be carefully balanced when offered to naïve users, as the quantity of information might be too much for them to process. A slower, step-by-step approach can be considered in such cases. This echoes the study from Blackwood-Brown et al. (2019)[10], who show that cybersecurity awareness of senior citizens can be improved through face-to-face classes and hands-on training workshops. Senior citizens with years of internet use were found to be as competent as younger individuals, but others mentioned that the single training session of 2 hours was too short to absorb and process all the information.

---

[7] R. Shillair, S. Cotten, H.-Y. Tsai, S. Alhabash, R. Larose, and N. Rifon. Online safety begins with you and me: Convincing Internet users to protect themselves. Computers in Human Behavior, 48:199–207, 2015. doi: 10.1016/j.chb.2015.01.046.

[8] L. Zhou, B. Parmanto, Z. Alfikri, and J. Bao. A Mobile App for Assisting Users to Make Informed Selections in Security Settings for Protecting Personal Health Data: Development and Feasibility Study. JMIR MHEALTH AND UHEALTH, 6(12), Dec. 2018. ISSN 2291-5222. doi: 10.2196/11210.

[9] N. H. Abd Rahim, S. Hamid, and M. L. M. Kiah. Enhancement of cybersecurity aware- ness program on personal data protection among youngsters in Malaysia: an assessment. Malaysian Journal of Computer Science, 32(3):221–245, 2019. ISSN 0127-9084. doi: 10.22452/mjcs.vol32no3.4.

[10] C. Blackwood-Brown, Y. Levy, and J. D'Arcy. Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective. Journal of Computer Information Systems, 2019. doi: 10.1080/08874417.2019.1579076.

Summary

As this field of research grows larger, there will be a bigger necessity for generic, reliable, objective effectiveness assessment methods. As a part of this objective, a clear line needs to be drawn between information security awareness and cyber behaviour. It is not simple how these things affect one another; for example, does high information security awareness necessarily implies safe cyber behaviour? Looking into such matter should help orienting the research in the right direction. Another suitable step forward would be to explore the literature in the UK Computing Education field to gain a deeper understanding into the various measures and methods that have proven successful in teaching technical knowledge to a variety of ages, levels of understanding, and accessibility requirements.

All authors are members of the Centre for Doctoral Training in Cybersecurity, University College London, United Kingdom.

Hawra Milani – h.milani@ucl.ac.uk
Sergi Bray – sergi.bray.18@ucl.ac.uk
Antoine Vendeville – a.vendeville@ucl.ac.uk

Funder information

This project was funded by the UK EPSRC grant EP/S022503/1 that supports the Centre for Doctoral Training in Cybersecurity delivered by UCL's Departments of Computer Science, Security and Crime Science, and Science, Technology, Engineering and Public Policy.