Human Factors in Cybersecurity, Vol. 53, 2022, 120–127
https://doi.org/10.54941/ahfe1002209

From Security-as-a-Hindrance Towards User-Centred Cybersecurity Design

Rick van der Kleij[1,2]

[1]The Hague University of Applied Sciences (THUAS), The Hague, The Netherlands
[2]The Netherlands Organisation for Applied Scientific Research (TNO), The Hague, The Netherlands

ABSTRACT

Cybersecurity controls in the workplace are viewed by many people as a hindrance that results in wasted time. End-users often bypass controls to get their work done and because of this, even the technically most secure systems can become unsecured. One crucial reason for this could be a lack of attention paid to usability factors by the software development teams that design controls. In this paper I investigate how to design cybersecurity controls in such a way that the user is more likely to behave in a secure manner when confronted with these controls. I put forward three practices that, when employed alongside each other, hold the promise to produce usable and effective cybersecurity controls.

Keywords: Usable security, Human-centred design principles, Choice architecture, Security awareness, Cybersecurity controls

INTRODUCTION

Security controls are important in keeping organisations safe from external threats to their cybersecurity. These controls help to reduce or mitigate the risk to the organisation's assets, such as customer data and information systems. Security controls can be classified according to their characteristics in up to 18 different families (Bodeau & Graubart, 2013). Examples include access control, awareness and training, incident response, and physical and environmental protection. Security controls in the workplace are however only effective when used correctly (Whitten & Tygar, 1999), and therefore do not automatically lead to improved security (Sasse & Flechais, 2005; Furnell, 2005) especially when they concern or involve the end-users of the IT systems that should be kept safe. Controls that involve the end-user focus on influencing behaviour among the workforce to help them become more security-aware or more skilled in reducing the cybersecurity risk to the organisation. An example is password management; employees are usually required to use strong passwords, not share passwords amongst each other, use password managers to keep their passwords safe, and not reuse passwords across applications and services.

From a technical security perspective, cybersecurity controls that focus on the behaviour of the end user are sensible measures to improve the organisation's security maturity. Strong passwords, for instance, take longer time

to crack than simple ones. However, when we look at these controls from a human factors perspective, there are often some serious flaws (Furnell, 2005), and as a consequence people have problems using the security controls correctly (Sasse & Flechais, 2005; Seiler-Hwang et al., 2019). For instance, Whitten and Tygar (1999) demonstrated that people with a good level of technical knowledge, even after receiving instructions and practice, failed to use security controls correctly. Often the controls that cause these problems do not acknowledge human characteristics, such as working memory limitations (Farrington, 2011), or the fact that humans are not rational entities (as computers) that act on knowledge alone (Sligo & Jameson, 2000). It is even imaginable that end-users intentionally destruct or turn off the controls that hinder them in doing their work. This phenomenon could be seen as an example of warning fatigue that can result from being 'overwarned' (Bliss, 1993). The term is used to describe situations where end users who are exposed to recurring warning messages about a security risk, which then does not eventuate, become cynical, apathetic and 'tired' of hearing warnings. They may become desensitized to the risk, thereby endangering themselves even more or sabotaging the system responsible for the warning messages. In this manner even the most secure systems can become unsecured (Feth & Polst, 2019).

The failure of cybersecurity controls could also be attributed to a conflict between two incompatible goals, namely completing one's work in time or keeping it safe (Stroebe, 2013). The efficient execution of tasks that help users attain their goals take priority. Security controls enable the execution of the tasks that help users attain their goals in the longer term but are not essential in achieving these goals (Sasse & Flechais, 2005). Therefore, people may view security controls as a hindrance. For instance, almost half of the office workers surveyed by Weigand agreed that security controls results in a lot of wasted time. More than half of the office workers were more concerned about deadlines than exposing the business to a data breach. Nearly a third of them had even tried to circumvent security measures (Weigand, 2021).

Stroebe and colleagues (2013) presented a model in order to understand the difficulty that people have in attaining two incompatible objectives. According to this model, explaining why even motivated dieters fail to succeed in their weight loss goal, dieters fail in food-rich environments because of surrounding food cues that strongly prime the aim of eating enjoyment. This conflict is exacerbated by the fact that these goals are incompatible. When transposed to the cyber realm, it could well be that although people are motivated to behave securely they fail to do so because they are surrounded by work cues, such as deadlines, that prime the goal of completing the work in a most efficient manner. The fact that it takes extra time and effort to comply with data security policies makes these two goals incompatible. Hence, if security is too cumbersome then an easier route could be realised to achieve work related goals. For instance, when mandatory secure applications hinder people in doing their work, applications not yet sanctioned by the IT department and therefore potentially harmful to security could be used.

Yet another reason why users can fail to comply with cybersecurity controls is that the required security behaviour is awkward or conflicts with the image that users want to present to the outside world (Sasse & Flechais, 2005). An example is locking the screen in the presence of colleagues when leaving the workplace, even for brief periods. If controls require users to behave in a manner that conflicts with their norms, values or self-image, most users will not comply. In addition, the environment surrounding the process of developing security and the culture in the workplace can influence the information security compliance levels of end users. For instance, the enthusiasm of higher management towards security by setting examples or modelling appropriate behaviour, or with their presence in the cybersecurity control design process, can all impact security design and use of controls in great ways (Sasse & Flechais, 2005).

An explanation for the abovementioned flaws in the design of security controls could be a lack of attention to usability factors in the design process. Although attention to security is an important issue in software development teams, and developments such as 'shift-left testing' are becoming common practice, human factors insight is often not part of the team members' skillset. Through human-centred approaches, applied early on in the security control development process, it is perhaps possible to tackle this problem of unusable security controls. This should enable the users confronted with these controls to behave in a more secure manner, or even prevent unsafe behaviour. When issues are addressed during the security control development process, rather than later once the control is being used, problems that could potentially cause damage through unsafe behaviour are avoided.

The design challenge to achieve satisfactory cybersecurity controls requires an interaction where people, process and technology complement each other rather than get in each other's way. In the remainder of this paper I investigate how to design security controls in such a way that the user, when confronted with these controls, is more likely to behave in a secure manner. I discuss human-centred design characteristics and techniques such as nudging and opportunity regulation, and how these can be integrated in a user-centred design approach for usable cybersecurity.

USER-CENTRED SECURITY DESIGN: THREE PRACTICES

User-centred security design is the application of social sciences knowledge into the design of security measures. The aim of this design philosophy is to create security systems in such a way that the users are more likely to behave in a secure manner (Van Steen & De Busser, 2021). Besides the obvious, —to include human factors specialists in software development teams who understand the meaning of usability and engage users early in the design process when designing security solutions, —I put forward three further practices in this paper. When employed alongside one another, these practices hold the promise to produce secure controls that are workable in practice and prevent users from being the 'weakest link'. The practices that increase the security level of any system are the following: to reduce the knowledge level required for using controls; to provide for better opportunity to behave more safely;

and to influence the motivation to use the controls in the required manner. These three practices will be examined in more detail but first I will briefly discuss Michie's et al. (2011) Capability Opportunity Motivation-Behaviour model (COM-B) to provide a suitable background.

COM-B states that people's behaviour can be explained by their capabilities, opportunity, and motivation. Capabilities are defined as the psychological and physical capacity of the individual to exhibit specific behaviour, including having the necessary knowledge and skills. Opportunity is defined as being all factors that lie outside the individual that make or prevent behaviour, such as the influence that our environment and the people around us can have on our choices. Motivation is defined as all the brain processes that activate and direct behaviour. The three user-centred security design practices discussed in this paper are based on these three determinants of behaviour.

The first practice I want to put forward, related to Michie's et al. (2011) psychological capability construct, is to decrease the knowledge requirements for using security controls. The efficiency of present-day security controls relies heavily on the knowledge that is required to operate them (Besnard & Arief, 2004). Practices aimed at increasing the efficiency are usually in the form of training and educational tools for end-users. It is anticipated that users' knowledge on how to use the security control would mature to satisfactory levels through security awareness campaigns, teachings, security policies and other methods. It often has little effect however, especially in the longer term (Bada et al., 2015), partly because of the loose coupling between the training and the actual use of the security control. Employees often know that there are security policies and have undertaken basic awareness training including good password practice; however when the time comes to change their password, the practice is long forgotten. For this reason we need to lower the knowledge requirements for using the control and to make this knowledge available at the time it is needed to trigger a successful application of the required security behaviour (Parkin et al., 2019; Fogg, 2009). For instance, when users are prompted to change their password for an application or service, this trigger is used to explain why this is necessary, how to make a strong password and keep it safe, and why one should never reuse passwords between applications (Habib et al., 2017; also figure 1).

The second practice, targeted at the factors that lie outside the individual, is to provide a better opportunity to behave safely or discourage unsafe behaviour. We should try to make it easier for people to behave in the desired manner by better supporting people's business goal-oriented behaviour in the design of security controls. An example of this practice is the fingerprint authentication procedure to gain access to devices or services. Contrary to the use of a password or passphrase as a control measure to gain access, the fingerprint is unique, almost always available and impossible to forget, making it the better authentication option by far. It should be noted, however, that a good, strong password is more secure than fingerprint authentication. Fingerprints cannot be altered if they are compromised, nor can they be altered between different accounts or devices (Sellers, 2017). Furthermore, fingerprint scanners can be easily hacked, even with everyday items such as wood glue (KrakenFX, 2021). Another example of how to provide a better opportunity to behave

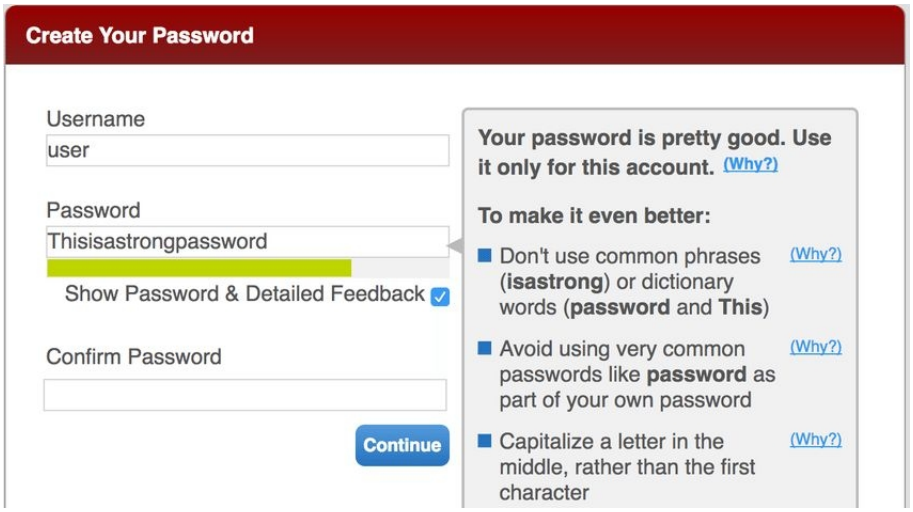

Figure 1: Example of how to decrease the memory burden to use security controls: Bullet point feedback at the time it is needed (Habib et al., 2017).

safely is the integration of privacy screens in the design of laptops. To deter so-called 'visual hacking', which consists of looking over someone's shoulder to gather information and credentials, people can place a privacy screen in front of their laptop screen when working in public places. However, these screens are often forgotten. By integrating them into the design of the laptop with a touch of a button the user can instantly mask their display, making it more easy to behave in a cyber-secure and compliant manner (Whittaker, 2018; see also figure 2).

The second practice is closely related to techno-regulation, a subfield of law, which suggests that security can be forced by taking away the freedom to act differently (Van Steen & De Busser, 2021; Leenes, 2011). This means not merely making it easier for people to behave in the desired manner, but preventing end-users from doing anything that is not the preferred option from the security control developers' point of view. Hence, techno-regulation offers opportunities to have policy enforced in a strict sense. The major upside is that behaviours that would lead to cyber insecurity are not possible to perform. This leads to an interesting issue. Should regulated users be able to work around, neglect or ignore prescribed policies? Strict techno-regulation may completely sidestep the moral dimension of cybersecurity, and although not complying with regulations reduces monitoring possibilities and the overall security of the system, a security culture is more than orders backed by threat.

The third practice, related to Michie's et al. motivation construct, is to influence by interface design people's behaviour by restructuring their presented choices. This refers to the concept of 'nudging'. The goal of this practice is to motivate end-users, from a security perspective, to make the preferred choice via the design of the security control. While forcing people's decisions towards the desired outcome through technology regulation could create reactance, nudging aims to be perceived as less paternalistic, while

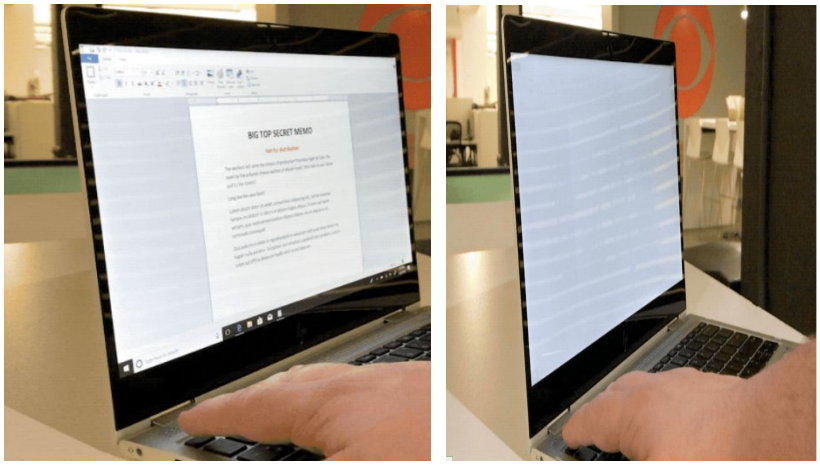

Figure 2: Example of how to design for better opportunity: Built-in privacy screen.

Figure 3: Example of nudging in the direction of good security practice: Password strength meter (Sundar, 2020).

protecting freedom of choice (Hartwig, & Reuter, 2021). People are not obligated to use security controls and unsafe alternatives are not removed, but the options are presented in such a way that the preferred option is more likely to be chosen (Van Steen & De Busser, 2021; see also figure 3).

Hartwig and Reuter (2021) found that nudging in cybersecurity is perceived as being helpful as long as the nudges are transparent, sources are trustworthy, and they appear only occasionally. Sharma and colleagues (2021) found that digital nudging in the form of priming users to information security risks is an effective way to reduce users' exposure to cybersecurity risks. They concluded that the use of instance-based information to prime tech-savvy adult users on potential security risks can lead them into taking safer security actions. Although these results seem promising, it is important to keep in mind that nudging usually does not lead to a 100% compliance rate. It does ensure, however, that the way in which choices are offered is the optimal method from the choice architect's point of view, leading to the highest level of compliance without the need for punishment, or restriction of freedom of choice (Van Steen & De Busser, 2021).

CONCLUSION

I started this contribution with the observation that cybersecurity controls do not often work as intended, especially when they concern or involve the end-users of the IT-systems that need to be kept safe. These end-users have other tasks to perform rather than spend their work time on securing the systems they work with and the information they produce. If controls are not usable enough and weigh users down, and the task of protecting the IT systems is considered to be in the way of the completion of other tasks, users will probably find ways around them. Understanding the factors that hinder the adoption of cybersecurity controls can allow for the redesign of practices that help end-users become better equipped to reduce the cybersecurity risk to the organisation. Making cybersecurity controls easier to use is a good starting point to ensure that it is as easy to work securely as it is to work unsecured. As a first step in this direction, I have adapted Michie's (2011) COM-B model to the design of controls. I derived three practices from this framework: (1) to lower the knowledge requirements for using the control and to make this knowledge available at the time it is needed to trigger a successful application of the required security behaviour; (2) to provide for better opportunity to behave safely or discourage unsafe behaviour; and (3) to influence the choice architecture to lead end-users into taking safer security actions. In my opinion the best practice to increase the usability of cybersecurity controls is an integrated approach, using the three practices as discussed in this paper alongside each other and complementary to other human-centred design principles. Until this happens, the many cybersecurity incidents that organisations continuously experience and the reputational and financial damage caused by them will be a reminder that effective cybersecurity control design needs to find the balance between the needs of security and the needs of the end-user.

REFERENCES

Bada, M., Sasse, A., & Nurse, J. R. C. (2015) Cyber security awareness campaigns: Why do they fail to change behaviour? In: International Conference on Cyber Security for Sustainable Society.

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security, 2004*, 23(3), 253–264.

Bodeau, D., & Graubart, R. (2013). Cyber resiliency and NIST special publication 800-53 rev. 4 controls. *MITRE, Tech. Rep.*

Bliss, J. P. (1993). The cry-wolf phenomenon and its effect on alarm responses.

Fogg, B. J. (2009). A behavior model for persuasive design, in Proceedings of the 4th international Conference on Persuasive Technology. ACM, 2009, p. 40.

Farrington, J. (2011). Seven plus or minus two. *Performance Improvement Quarterly*, *23*(4), 113–116.

Feth, D., & Polst, S. (2019). Heuristics and models for evaluating the usability of security measures. In *Proceedings of Mensch und Computer 2019* (pp. 275–285).

Furnell, S. (2005). Why users cannot use security. *Computers & Security*, *24*(4), 274–279.

Habib, H., Colnago, J., Melicher, W., Ur, B., Segreti, S., Bauer, L., ... & Cranor, L. (2017). Password creation in the presence of blacklists. *Proc. USEC*, 50.

Hartwig, K., & Reuter, C. (2021, October). Nudge or Restraint: How do People Assess Nudging in Cybersecurity-A Representative Study in Germany. In *European Symposium on Usable Security 2021* (pp. 141–150).

KrakenFX (2021, November 19). Your Fingerprint Can Be Hacked For $5. Here's How. https://blog.kraken.com/post/11905/your-fingerprint-can-be-hacked-for-5-heres-how/.

Leenes, R. (2011). Framing techno-regulation: An exploration of state and non-state regulation by technology. *Legisprudence*, *5*(2), 143–169.

Michie, S., Van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science, 42* (6). https://doi.org/10.1186/1748-5908-6-42.

Parkin, S., Redmiles, E. M., Coventry, L., & Sasse, M. A. (2019). Security when it is welcome: Exploring device purchase as an opportune moment for security behavior change. In *Proceedings of the Workshop on Usable Security and Privacy (USEC'19)*. Internet Society.

Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? In: Cranor, LF and Garfinkel, S, (eds.) Security and Usability: Designing secure systems that people can use. (13 - 30). O'Reilly: Sebastopol, US.Sellers, M. (2017). Don't Give Them the Finger: Why Passwords Are More Secure Than TouchID. Cryptography. https://derekbruff.org/blogs/fywscrypto/practical-crypto/dont-give-them-the-finger-why-passwords-are-more-secure-than-touchid/

Sharma, K., Zhan, X., Nah, F. F. H., Siau, K., & Cheng, M. X. (2021). Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity. *Organizational Cybersecurity Journal: Practice, Process and People*.

Seiler-Hwang, S., Arias-Cabarcos, P., Marín, A., Almenares, F., Díaz-Sánchez, D., & Becker, C. (2019, November). " I don't see why I would ever want to use it" Analyzing the Usability of Popular Smartphone Password Managers. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1937-1953).Sundar, S. (2020, June 30). Nudging towards a Secure Containerised Environment. TechBlog. https://medium.com/axel-springer-tech/nudging-towards-a-secure-containerised-environment-f4d6c08a253

Sligo, F. X., & Jameson, A. M. (2000). The knowledge-behavior gap in use of health information. *Journal of the American Society for Information Science*, *51*(9), 858–869.

Stroebe, W., Van Koningsbruggen, G. M., Papies, E. K., & Aarts, H. (2013). Why most dieters fail but some succeed: A goal conflict model of eating behavior. *Psychological Review*, *120*(1), 110.

Van Steen, T. & De Busser, E. (2021). Security by behavioral design: A rapid review. Technical report. Leiden University.

Weigand, S. (2021, September 9). Younger remote workers see security as a hindrance. SC media. Retrieved from the internet on January 24, from https://www.scmagazine.com/news/training/younger-remote-workers-see-security-as-a-hindrance.

Whittaker, Z. (2018). HP Spectre x360 has a built-in instant privacy screen. ZDNet. (January 15, 2018). https://www.zdnet.com/article/hp-spectre-x360-built-in-instant-privacy-screen/#:~{}:text=HP's%20Spectre%20x360%2C%20launched%20in,is%20an%20integrated%20privacy%20screen.

Whitten, A., & Tygar, J. D. (1999, August). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *USENIX security symposium* (Vol. 348, pp. 169–184).