H. Roßnagel, C. H. Schunck, S. Mödersheim, D. Hühnlein (Hrsg): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 83

On the diffusion of security behaviours

An informed argument using diffusion of innovations theory on the uptake of four different security behaviours

Sebastian Kurowski, Heiko Roßnagel[1]

Abstract: Security behaviour has been researched from a variety of theoretical lenses, however a clear picture on the factors that foster secure behaviour is still missing. This contribution uses the diffusion of innovations theory and applies it to four exemplary security behaviours to identify how it can explain the uptake of each behaviour. In contrast to many other approaches, it focuses on the behaviour itself, not the behaving individual. We are able to show differences in the uptake of idealized security behaviours. A perceived relative advantage positively impacts the uptake of a behaviour, however this advantage seems rarely to be motivated by a perceived risk. Risk only seems to play a minor role for the diffusion of security behaviours. Additionally, the relative advantage does not seem to be a necessity for the diffusion of a behaviour. If the other properties namely compatibility, triability, observability, and low complexity of a behaviour are adequately fulfilled a successful diffusion is still possible.

Keywords: Security behaviour; Policy Compliance; Diffusion of Innovation; Security Culture

1 Introduction

Secure behaviour is an important asset in an information security architecture. And while there has been a multitude of studies on secure behaviour, policy compliance, and policy adherence, there is to date no settled theoretical foundation [So15a], and thus no reliable guidance on how to foster secure behaviour in organizations. Additionally, recent findings suggest that the effect of training and awareness on the organizations security may be limited [Kw19]. Still human behaviour remains an important antecedent for security attacks [Jo16]. Some security behaviours seem to be picked up more easily than others' by individuals. Which leads to an interesting question: Why? Behavioural research in security tackles this question mostly by considering the behaving individual, with limited success so far [So14][So15a][Ku19]. However, there is little research on the impact of the security behaviour itself on its adoption rate. In order to shed light on this, we employ the theory on diffusion of innovations [Ro03] to security behaviours in order to discuss potential adoption successes or failures of secure behaviours. By doing so, we reduce the individual and its characteristics from the consideration, which makes sense if secure behaviour is considered an ideal behaviour, idealized by security experts.

[1] Fraunhofer-Institute for Industrial Engineering IAO, Team Identity Management, Stuttgart, 70599, firstname.lastname@iao.fraunhofer.de

This contribution includes a brief summary on the existing research on secure behaviour along with a brief discussion of its methodological constraints (Section 2.1), an introduction of the application of diffusion of innovations theory in security research (Section 2.2), followed by an overview on diffusion of innovations theory itself (Section 2.3). In order to approach the research question, we analyse four different security behaviours in the context of diffusion theory: employing privacy screens, covering the device camera, using e-mail encryption, and using single sign-on systems. We then use a Google Trends analysis on these behaviours in order to see which behaviours show an increasing interest, and which behaviours do not. We conclude with a summary of the diffusion properties of these behaviours (see Section 3). Of course, this contribution uses limited methodology, and informed arguments in order to draw its conclusion. Therefore, this research has mentionable limitations (see Section 4). However, our discussion will argue the practical relevance, and the epistemological appropriateness of our approach (Section 5).

2 Related Work

2.1 Security Behaviour

Secure behaviour has been approached from a variety of theoretical lenses, including value-focused (e.g. Theory of Planned Behaviour, TPB), rationality-focused (e.g. Rational Choice Theory, RCT), deterrence-focused (e.g. Protection Motivation Theory, PMT, and General Deterrence Theory, GDT), and environment-focused (e.g. Social Cognitive Theory, SCT) theories. For instance, the theory of planned behaviour (TPB) highlights that before we can expect actual secure behaviour, we need to induce the intention to act. That in turn relies heavily on the personal goal system, the external environment as well as the perceived personal ability to take control over the situation. TPB is founded in socio-psychology and combines individual and environmental aspects for explaining secure behaviour. It is used in various quantitative studies on secure behaviour [Sa15][Si14][So15b]. Rational choice theory is usually seen as evaluating the cost-benefit situation of non-secure behaviour, waging of sanction or consequence severity, and detection probability [If16][VS12] or waging of benefits of non-secure behaviour versus the costs of secure behaviour [Bu10][Ka13]. Quite contrary to the TPB, the subject actively wages off benefits versus costs of the situation and decides upon the maximum utility for itself. This view on rationality aligns well with the use of sanctions versus the benefits of a non-secure behaviour and is used accordingly [If16][Ka13][VS12]. PMT offers a foundation of secure behaviour that can be quite intuitive. After all, why should there be any other reason for individuals to exhibit secure behaviour, rather than averting a threat? PMT is therefore quite extensively used in quantitative studies on both secure and non-secure behaviours [Bo15][Jo16][Po15][PH14][Si14][So15a]. Social Cognitive Theory employing research stems from a theoretical foundation, where successful adaption of secure behaviour benefits from a social system that promotes and rewards and

where one gains experiences both by observing role models as well as engaging in activities raising their self-efficacy [GY12][Rh09]. Finally, general deterrence theory is a possible useful model for explaining why people adhere to rules and policies. Its focus aligns very well with possible considerations around secure behaviour. Similar to PMT the intuitive cause of secure behaviour should be the aversion of a threat, in this case the deterrence of a threat or punishment. Therefore GDT, such as PMT is widely used in quantitative studies on secure information security behaviour and the lack thereof [If16][Jo16][Li14]. All these approaches have in common that they try to explain secure behaviour in individuals. However, meta-analyses find no clear winner among these theoretical foundations [So15a]. Additionally, some of those quantitative studies show response biases [Ku19]. In addition, if one considers that research on secure behaviour mixes ideals with observable realities, namely something that security experts consider an ideal behaviour with actual behaviours by people mostly outside of the security domain, then the whole approach of researching the individual along with an idealized behaviour is questionable. Secure behaviour means that an individual is ought to behave in an idealized way, a „secure way". This however may collide with the individuals reality, which may be very different from the reality of a security researcher. If secure behaviour is considered an ideal, whereas behaviour itself is considered an empirically observable reality, then the observation of ideal versus behaviour can only be employed with epistemologies that do not reduce the social relationship between researcher and observation, such as interpretivism [Wa93]. One conclusion of this thought could be that secure behaviour should be approached with methodologies that are able to reflect the researcher in the observation. Another conclusion could be to focus on the idealized behaviour itself, rather than the individual and an idealized behaviour in conjunction. This contribution takes the latter path, by considering the diffusion of behaviours and thus how likely a behaviour is being picked up, and not how likely an individual may pick up a certain behaviour.

2.2 Diffusion of Information Security

The adoption and diffusion of information technology has been well researched in the economics and information systems domains. This has led to the development of widely accepted and used theories such as the diffusion of innovations theory [Ro03] and the technology acceptance model [Da89]. In information security research, however, these theories have only been used very rarely. [RZ12] proposed a structured approach to assess market success of information security technologies based on the Diffusion of Innovations process. They also applied this approach to several technologies such as electronic signatures [Ro06], privacy enhancing technologies [Ro10] and federated identity management [Hü10]. However, to the best of our knowledge it has not yet been applied to security behaviour, which is surprising, as security behaviour can be considered as an innovation just as likely as technology.

2.3 Diffusion of Innovations

This research examines a variety of factors, which have been shown to be determinants of IT adoption and usage, and further has been applied to explain the adoption and diffusion of a great variety of innovations ranging from new methods of agriculture to modern communication technology. In his seminal work Rogers defines five attributes of innovations, as perceived by the members of the social system that determine the rate of adoption of an innovation [Ro03]: Relative Advantage, Compatibility, Complexity, Triability and Observability.

Relative advantage is the degree to which an innovation is perceived as better than the idea it supersedes. It is not so important if the innovation has an objective advantage, but rather if the individual perceives the innovation as advantageous. Advantages can be measured in economic terms, but social prestige, convenience, and satisfaction also can play an important role. **Compatibility** is the degree to which an innovation is perceived as being consistent with the existing values, past experiences, and needs of potential adopters. An Innovation that is consistent with the existing values will diffuse more rapidly than one that is incompatible with the norms and values of the social system. **Complexity** is the degree to which an innovation is perceived as difficult to understand and use. Innovations that are easier to understand will be adopted more rapidly than those which require the adopter to develop new skills and understandings. **Triability** is the degree to which an innovation may be experimented with on a limited basis. New ideas that can be tried before the potential adopter has to make a significant investment in the innovation are adopted more quickly. **Observability** is the degree to which the results of an innovation are visible to others. The easier it is for individual to observe the results of an innovation, the more likely they are to adopt [Ro03]. In addition to the main attributes, Rogers also describes the diffusion process: ”The innovation-decision process is the process through which an individual passes from gaining initial knowledge of an innovation, to forming an attitude toward the innovation, to making a decision to adopt or reject, to implementation of the new idea, and to confirmation of this decision” [Ro03]. The start and speed of the innovation-decision process varies between the different members of the social system. Therefore, the various decisions to adopt or reject the innovation are also spread over time. The dynamic of this process is a result of the changes in the information the individual acquires and possesses about the innovation [Li00].

3 Diffusion properties of security behaviour

In the following we are going to apply the diffusion of innovations theory to several exemplary security behaviours. We will discuss how it can explain the successful adoption of each behaviour.

3.1 Privacy Screen Protector

Shoulder surfing is a low cost attack that can be utilized easily, especially with mobile users [Lo11]. An effective deterrent against these kinds of attacks are privacy screen protectors, which reduce the possible angle of view on the device screen. This way, only individuals that are at the right angle with regard to the device are able to see the screen contents. **The risk:** The risk of shoulder surfing is quite tangible. Unlike other information security threats, materialization of this risk does not require some virtual, invisible attacker. In fact the risk of shoulder surfing can become tangible, in principle, as soon as one spots someone else, who is looking at one's device screen. However, apart from social engineering enthusiasts and security experts, the risk of shoulder surfing is seemingly not perceived as an existing one [Ha14][Tr16].**The impediments:** Privacy screens darken the device screen, and inhibit individuals to one's left or right to look at the screen. This means that there could be a major work impediment for individuals who rely on physically sharing their screen. However, especially in times of mobile work, physically sharing the screen becomes less and less likely as remote work increases. Furthermore, the screen can easily be removed if needed. **The countermeasure:** A screen protector is tangible and easy to understand. Its effects are visible as soon as it is applied. Finally, it is removable and can therefore be tried out. **Assessing the diffusion:** Summing up, the privacy screen protector could provide a *relative advantage* by providing felt security. However, in light of the lack of risk perception it is questionable as to how a relative advantage can be perceived through this. On the other hand a perceived relative advantage could be reduced if physical sharing of a device screen is required, but especially with the rise of mobile work, it is disputable as to what extent this influences the relative advantage of screen protectors. The solutions *compatibility* again depends largely on the requirement to physically share a device screen, which we expect to be relatively seldom. The solution is easy to understand (low *complexity*), its application can be observed (*Observability*), and it can be tried out easily (*Triability*). Due to the lack of relative advantage of applying screen protectors, we would expect this behaviour to not be widely adopted. However, as Figure 1 shows, the opposite is the case. Applying screen protectors shows slowly, but increasing interest according to Google Trends.

Relative Advantage	Compatibility	Low Complexity	Observability	Triability	Expected Adoption Speed
✕	■	■	■	■	Moderate

Table 1 Diffusion properties of applying screen protectors. (■ = Given, ○ = Conditionally given, ✕ = Not given)

3.2 Encryption of E-Mails

E-Mail encryption is the only effective countermeasure against passive and active Man-in-the-middle (MitM) attacks. Since E-Mails are inherently insecure, unauthenticated and not confidential, everyone who is involved in sending a mail can read and change the contents. By encryption of the mail, breaches of the mails contents confidentiality can be avoided, and the authenticity and integrity of contents can be ensured. **The risk:** Perceived risks of emails seem to influence user attitudes towards emails only minimal [Ch11]. This is unsurprising given findings whereas a man-in-the-middle, or the risk of confidential information being disclosed to untrusted networks are among the lowest perceived security risks [Tr16]. **The impediment:** The work impediment of encrypting e-mails can be substantial. After all, additional software, configuration, certificate management and credentials are required. This process provides numerous pitfalls for users, which themselves have led to security vulnerabilities in the past [Sh06]. **The countermeasure:** Commercial and non-commercial encryption solutions are not developed with the user experience in mind. Although they can be obtained easily, users must still achieve a certain level of security literacy. For instance in order to use PGP, one must understand the difference between a public and a private key certificate, and how to use the certificate server and its trust evaluations. **Assessing the diffusion:** The *relative advantage* of email encryption largely depends on the perceived risk of a Man-in-the-Middle. However, it seems that this risk is usually not perceived to be a major concern. Therefore, the relative advantage of email encryption seems to be very low. *Compatibility* of the solutions should be low, as processes require additional steps, and additional literacy is required to even use the solutions. Likewise, the *complexity* of encrypting emails is high. The encryption itself however is visible (*Observability*), however, the effects of encrypting emails can never be observed, since the threat is a virtual and non-tangible one. Finally, email encryption requires obtaining additional literacy, installation and configuration of additional tools. These perceivable hurdles stand against the *triability* of encrypting emails.

Relative Advantage	Compatibility	Low Complexity	Observability	Triability	Expected Adoption Speed
×	×	×	×	×	Slow, if at all

Table 2 Diffusion properties of encrypting emails. (■ = Given, ○ = Conditionally given, × = Not given)

3.3 Covering of the device camera

Threats that use the device camera, for instance privacy breaches by Facebook [Go20], or government institutions have been publicly visible through various media reports and the Snowden leaks. Besides of physically deactivating the camera, a possible avoidance tactic for this could be the taping of the devices camera. Hereby a tape is applied, which cannot

be seen through. It renders the camera virtually useless. **The risk:** As to our knowledge there is no study available that measures the perceived risk of being spied on through the device camera. However, there are studies that involve cameras in smart homes which show that users tend to be more aware of their own behaviour, and some even more cautious because they were feeling observed by the cameras in their smart home devices [Ta19]. Therefore, it seems reasonable to assume that the risk of being spied on through the device camera is perceived as a likely and tangible one by individuals. **The impediment:** The camera in devices can be useful for selfies and video conferences. In that case, simply covering the camera would be an impediment, as the cover always has to be removed prior to the selfie, or prior to the conference. On the other hand, there are camera covers available, which can be opened and closed, drastically reducing the possible impediment. **The countermeasure:** Covering the camera is a tangible action, whose consequences can be seen immediately. When the camera is covered, individuals will notice that they only see a dark image when using the camera. Additionally, camera covers are relatively easy to obtain and can be applied without additional security literacy. **Assessing the diffusion:** The relative advantage seems to build on a tangible and perceived risk. However, if the camera is heavily used the impediment of the camera covers can reduce or even eliminate the perceived relative advantage of the solution. Compatibility of the solution is high, since it can be applied without additional steps and to virtually any device camera. The behaviour is easy to understand (low *complexity*), can be observed with others (*Observability*). Finally, because the camera cover is easy to obtain, easy to apply, easy to remove, and its consequences easy to understand, it can be tried out well (*Triability*).

Relative Advantage	Compatibility	Low Complexity	Observability	Triability	Expected Adoption Speed
○	■	■	■	■	Moderate

Table 3 Diffusion properties of covering the device camera. (■ = Given, ○ = Conditionally given, ✕ = Not given)

3.4 Use Single-Sign-On systems

Single sign-on (SSO) system provide the possibility to reduce complexity and ease the use of credentials for users. They are an option to eliminate password reuse [Iv04], and weak passwords [Ne94]. Additionally, they offer the reduction of implementation complexity by standardizing application authentication interfaces, and the automation of access rights and authentication data provisioning and deprovisioning. **The risk:** Single sign-on addresses risks regarding passwords. However, we suspect that these risks are mostly perceived by individuals with a given security literacy. Apart from these, there are no further risks that are addressed by SSO. **The impediment:** The impediment is little, once SSO is available. Using SSO resembles the use of known credentials such as username and passwords. **The countermeasure:** While the technical implementation of SSO is

demanding, users are not necessarily required to obtain further security literacy in order to use SSO. Additionally, every application can, in principle, be integrated with SSO. Even in consumer areas, SSO services provided by Google and Facebook via protocols such as oAuth are available. **Assessing the diffusion:** SSO provides automation capabilities and solves a security risk. However, probably the biggest advantage of SSO lies in the standardization of interfaces and drastical reduction of required authentication procedures. Therefore, we assume that SSO will yield a high perceived *relative advantage*. While the *complexity* of the implementation can be challenging, the complexity of use is not. SSO can leverage already known authentication mechanisms such as username and password. The observability of SSO in terms of reduced authentication steps is observable (*Observability*). And since SSO is available in the consumer branch through Facebook and Google, it can be tried out (*Triability*).

Relative Advantage	Compatibility	Complexity	Observability	Triability	Expected Adoption Speed
■	■	■	■	■	Fast

Table 4 Diffusion properties of using SSO (■ = Given, ○ = Conditionally given, ✕ = Not given)

3.5 Security Behaviours and their diffusion properties

The analysis in the previous Subsections is summarized in the following Table 5. Hereby each behaviour is ranked, based on the Google Trends analysis shown in Figure 1 and Figure 2. The Google Trends analysis clearly shows that SSO has largely increased in interest over the last years, followed by a slower but steady increase in interest in privacy screen protectors (see Figure 1). The interest in camera covers has also steadily increased, although at a much slower pace as in the case of privacy screen protectors. Therefore, it is only visible in Figure 2. Hereby, the interest in camera covers has bypassed the interest in e-mail encryption since 2017, with a notable exception in May 2018 (the year where the European General Data Protection Regulation went into action). Against this, E-Mail encryption has steadily lost interest, since 2004. Notably the interest peaks only shortly in 2013, 2014, and 2018, whereas 2013 and 2014 mark the years of the Snowden revelations. In our opinion it is therefore safe to say, that the interest in E-Mail encryption, despite for short lapses of attention, is constantly decreasing, while the interest in camera covers increases. Additionally, one must take into account that all Trends Analyses are for topics, which comprise multiple search terms on a certain topic. Camera cover is the only search term that is included in the Google Trends Analysis. However, due to the higher specifity of the search term, interest should be lower than that measured for the respective topics. This however is not the case. Table 5 summarizes the diffusion properties of the different security behaviours. The assigned rank reflects the interest in the behaviour, according to Google Trends.

Behaviour	Rel. Adv-	Compatibility	Complexity	Observability	Triability	Rank
Use SSO	■	■	■	■	■	1
Screen protector	✕	■	■	■	■	2
Camera Cover	○	■	■	■	■	3
E-Mail Encryption	✕	✕	✕	✕	✕	4

Table 5 Overview on the diffusion properties of security behaviors (Rel. Adv. = Relative Advantage, ■ = Given, ○ = Conditionally given, ✕ = Not given). The rank orders the behaviours according to the interest in Google Trends with 1 being the highest interest, and 4 being the lowest.

As expected, the perceived relative advantage seems to contribute to the uptake of a behaviour, but not as dominant as for other innovations. The reason is the dependence of perceived relative advantage on perceived risks addressed by the security behaviour.

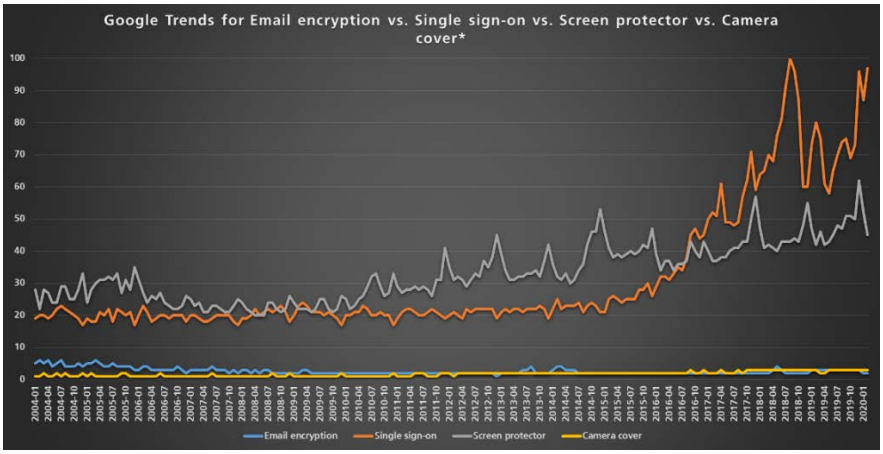

Figure 1 Google Trends for Email encryption, SSO, screen protector and camera cover. Camera cover is the only search term in the comparison, the others are topics

As those risks are often not recognized by users the relative advantage is very low. For privacy screen protectors, we cannot conclude a perceived relative advantage, in light of the relatively low perceived risk of shoulder surfing [Ha14][Tr16]. On the other hand, a relative advantage can only be expected for camera covers, if the camera is not heavily used. As a result, Compatibility, Complexity, Triability, and Observability seem to play a leading role with security behaviours. If a perceived relative advantage is not given individuals may still adopt a security behaviour. However, if it is hard to try out, if its

functions and consequences are not observable, and if it is not compatible with what one knows and does, it will likely fail in the long run, as the case of email encryption.

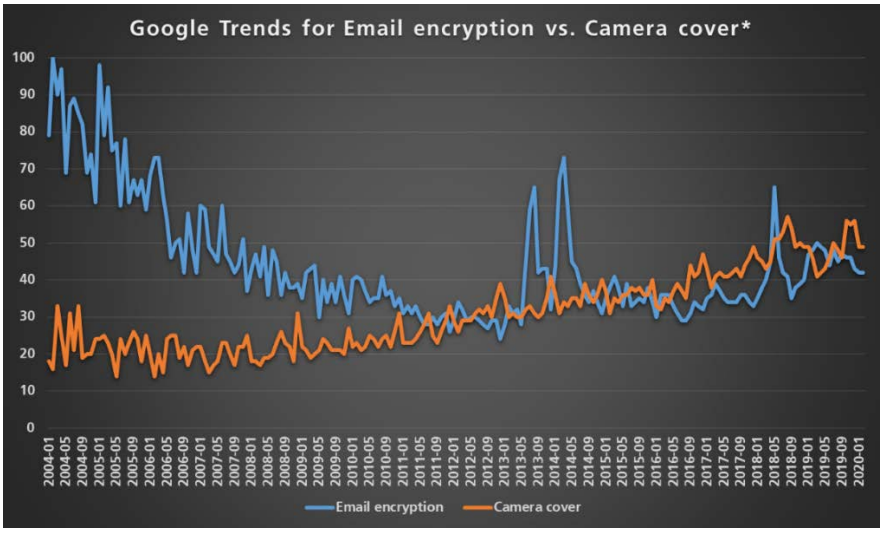

Figure 2 Google Trends for Email encryption and Camera cover. Email encryption is a Google Topic, whereas camera cover is only a search term

Risk on the other hand, does not really seem to play a role in the uptake of security behaviours. Even if a relative advantage could not be attributed to a risk that was actually perceived as a large one by individuals, the behaviour seems to still be interesting, if triability and observability are given, and the complexity of the behaviour is low. In light of the findings of [Kw19] however, this is hardly surprising as they find that awareness and security training only impacts an organizations security marginally.

4 Discussion and Impact

The results clearly show that diffusion theory can provide an explanatory framework for the likelihood of widespread adoption of certain security behaviours, and the absence thereof. It does not provide any insight into how to foster a certain secure behaviour with individuals. But it enables security experts to talk about behaviours which may make sense to include in an organizational policy or campaign, and which are likely to fail. Therefore, these results can provide a lasting impact on how security behaviour is approached in organizations. The findings align well with the observations on the diffusion of preventive innovations [Ro02], where the perceived relative advantage also tends to be generally lower. Rogers therefore proposes marketing the relative advantage of the innovation. However, while this may work well with health interventions, such as [LE00], one has to

be careful when applying this principle to information security. When perceived security risks constitute for an individuals perceived relative advantage, then the constitution is built on a constructed, anticipated event [Lu90] rather than a naturally occurring event such as a health disease. This shows that the epistemological discussion is in principle important for this research topic. In the end of Section 2.1, a discussion of secure behaviour research as research on actual behaviour in light of idealized behaviour was conducted. It led to the point that this kind of research should either focus on the idealized behaviour itself (which is what we did in this contribution), or employ epistemological focuses that do not separate between the idealist, the idea, and the observation (e.g. interpretivism [Wa93]). An important take away from interpretivism however is that quantitative methodologies that rely on the testing of fact rather than on interaction may not be useful after all. With other epistemological focuses that do not reduce the relationship of researcher and research, like phenomenology [Hu09], or constructivism [Lu84], generalizable methodologies and the transfer of knowledge between cases of research subjects itself even are questionable. In this field, the qualitative approach that is provided by diffusion theory is suiting, but not settled. Criticism on diffusion theory [LD01] can basically be reduced to a phenomenological approach or to the employment of radical constructivism. Therefore, this research seems to be on a good path and at least in the short term able to provide insights with value for security professionals on secure behaviour.

5 Limitations

There are several limitations to this contribution. It does not involve any empirical work besides Google Trends analyses. While the absence of quantitative empirical work makes sense due to the reasons laid out in Section 4, the absence of qualitative empirical work does not. We tried to scrutinize the different security behaviours as comprehensible as possible but the analysis drawn only represents our personal view. Google Trends is of course itself a biased research mechanism. It only measures queries by Google and not actual behaviours. Therefore, it can only provide an indication of the diffusion of a security behaviour under the assumption that individuals will inform themselves via Google about the behaviour. And especially with encrypting emails, the behaviour may be common knowledge. But then privacy screen protectors have been around nearly as long as email encryption. And for instance PGP, which has been around for around 30 years, still is “only” a niche product. Additionally, Google is the leading search engine around. Therefore, we believe the indications from Google Trends to be useful data in the context of this research.

6 Conclusion

By separating the idealized security behaviour, from the behaving individual we were able to provide an insight into why certain security behaviours are successful, while others are not. This research shows that the diffusion of innovations theory provides a framework

that enables a discussion and anticipation of the success of different security behaviours. As relative advantage is often rather small, it alone does not provide a safe bet, but seems to enhance the adoption of a behaviour. Necessary factors for a security behaviour to be successful however are the compatibility, triability and observability of the security behaviour. Risk does not seem to play major role in the uptake of security behaviours, which aligns well with the findings of [Kw19]. Of course, this research is limited regarding its use of informed arguments, and its reduction of the idealized security behaviours towards the adoption factors of diffusion theory. The use of Google Trends, while providing a good indication can also not be regarded as satisfyingly settling information on the adoption of security behaviours. Future research will employ qualitative methods in order to research best and worst cases of security behaviours in organizations to test the diffusion of theory framework. More scrutiny can be put into the cases of security behaviour, taking into account the environment and stakeholders that a security behaviour may involve, by employing perception-critical epistemological focuses such as interpretivism or radical constructivism.

Bibliography

[Bo15] Boss, S. et al.: What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. (2015).

[Bu10] Bulgurcu, B. et al.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. Management Information Systems Quarterly. 34, 3, 523–548 (2010).

[Ch11] Chen, R. et al.: An investigation of email processing from a risky decision making perspective. Decision Support Systems. 52, 1, 73–81 (2011).

[Da89] Davis, F.D.: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. Management Information Systems Quarterly (MISQ). 13, 3, 319–340 (1989).

[Go20] Goud, N.: Facebook to spy through your Webcam or Phone, https://www.cybersecurity-insiders.com/facebook-to-spy-through-your-webcam-or-phone/, (2020).

[GY12] Guo, K.H., Yuan, Y.: The effects of multilevel sanctions on information security violations: A mediating model. Information & Management. 49, 6, 320–326 (2012).

[Ha14] Harbach, M. et al.: It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception. In: 10th Symposium On Usable Privacy and Security (${$SOUPS$}$ 2014). pp. 213–230 (2014).

[Hü10] Hühnlein, D. et al.: Diffusion of Federated Identity Management. In: Freiling, F.C. (ed.) Sicherheit 2010. pp. 25–36 Köllen Druck + Verlag GmbH, Bonn (2010).

[Hu09] Husserl, E.: Philosophie als strenge Wissenschaft. Felix Meiner Verlag (2009).

[If16] Ifinedo, P.: Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines? Information Systems Management. 33, 1, 30–41 (2016). https://doi.org/10.1080/10580530.2015.1117868.

[Iv04] Ives, B. et al.: The Domino Effect of Password Reuse. Communications of the ACM. 47, 4, 75–78 (2004).

[Jo16] Johnston, A.C. a et al.: Dispositional and situational factors: Influences on information security policy violations. European Journal of Information Systems. 25, 3, 231–251 (2016). https://doi.org/10.1057/ejis.2015.15.

[Ka13] Kajtazi, M. a et al.: Assessing self-justification as an antecedent of noncompliance with information security policies. In: Proceedings of the 24th Australasian Conference on Information Systems. (2013).

[Ku19] Kurowski, S.: Response Biases in Policy Compliance Research. Information & Computer Security, Vol. ahead-of-print No. ahead-of-print. (2019). https://doi.org/10.1108/ICS-02-2019-0025

[Kw19] Kweon, E. et al.: The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. Inf Syst Front. (2019). https://doi.org/10.1007/s10796-019-09977-z.

[Li14] Li, H. a et al.: Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. Information Systems Journal. 24, 6, 479–502. https://doi.org/10.1111/isj.12037 (2014).

[LE00] Lock, C. A., Kaner, FS. E.: Use of marketing to disseminate brief alcohol intervention to general practitioners: promoting health care interventions to health promoters. Journal of evaluation in clinical practice. 6, 4, 354-357 (2000).

[Li00] Litfin, T.: Adoptionsfaktoren: Empirische Analyse am Beispiel eines innovativen Telekommunikationsdienstes. DUV, Wiesbaden (2000).

[Lo11] Long, J.: No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing. Syngress (2011).

[Lu84] Luhmann, N.: Soziale systeme. Suhrkamp Frankfurt am Main (1984).

[Lu90] Luhmann, N.: Technology, environment and social risk: a systems perspective. Organization & Environment. 4, 3, 223-231 (1990).

[LD01] Lyytinen, K., Damsgaard, J.: What's wrong with the diffusion of innovation theory? In: Working conference on diffusing software product and process innovations. pp. 173–190 Springer (2001).

[Ne94] Neumann, P.G.: Risks of Passwords. Communications of the ACM. 37, 4, 126 (1994).

[Po15] Posey, C. a et al.: The impact of organizational commitment on insiders motivation to protect organizational information assets. Journal of Management Information Systems. 32, 4, 179–214 (2015). https://doi.org/10.1080/07421222.2015.1138374.

[PH14] Putri, F., Hovav, A.: Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. In: ECIS 2014 Proceedings - 22nd European Conference on Information Systems. (2014).

[Rh09] Rhee, H.-S. et al.: Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security. 28, 8, 816–826 (2009).

[Ro03] Rogers, E.M.: Diffusion of Innovations. Free Press, New York (2003).

[Ro02] Rogers, E.M.: Diffusion of preventive innovations. Addictive behaviors 27, 6, 989-993 (2002).

[Ro06] Roßnagel, H.: On Diffusion and Confusion: Why Electronic Signatures Have Failed. Trust and Privacy in Digital Business. 71–80 (2006).

[Ro10] Roßnagel, H.: The Market Failure of Anonymity Services. In: IFIP. pp. 340–354 (2010).

[RZ12] Roßnagel, H., Zibuschka, J.: eID in Leisure Time Activities: Results from the SSEDIC Stakeholder Consultations in the Leisure Sector, (2012).

[Sa15] Safa, N.S. a et al.: Information security conscious care behaviour formation in organizations. Computers and Security. 53, 65–78 (2015). https://doi.org/10.1016/j.cose.2015.05.012.

[Sh06] Sheng, S. et al.: Why johnny still can't encrypt: evaluating the usability of email encryption software. In: Symposium On Usable Privacy and Security. (2006).

[Si14] Siponen, M. a et al.: Employees' adherence to information security policies: An exploratory field study. Information and Management. 51, 2, 217–224 (2014). https://doi.org/10.1016/j.im.2013.08.006.

[So15a] Sommestad, T. et al.: A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. International Journal of Information Security and Privacy (IJISP). 9, 1, 26–46 (2015).

[So15b] Sommestad, T. et al.: The sufficiency of the theory of planned behavior for explaining information security policy compliance. Information and Computer Security. 23, 2, 200–217 (2015). https://doi.org/10.1108/ICS-04-2014-0025.

[So14] Sommestad, T. et al.: Variables influencing information security policy compliance: a systematic review of quantitative studies. Information Management & Computer Security. 22, 1, 42–75 (2014).

[Ta19] Tabassum, M. et al.: " I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In: Fifteenth Symposium on Usable Privacy and Security (${$SOUPS$}$ 2019). (2019).

[Tr16] Trewin, S. et al.: Perceptions of risk in mobile transaction. In: 2016 IEEE Security and Privacy Workshops (SPW). pp. 214–223 IEEE (2016).

[VS12] Vance, A. a, Siponen, M. b: IS security policy violations: A rational choice perspective. Journal of Organizational and End User Computing. 24, 1, 21–41 (2012). https://doi.org/10.4018/joeuc.2012010102.

[Wa93] Walsham, G.: Interpreting information systems in organizations. John Wiley & Sons, Inc. (1993).