Security, Privacy and the “Human Factor”: Making Sense of the Paradoxes of Security and Privacy Behaviour

Spyros Kokolakis
Dept. of Information & Communication Systems Engineering, University of the Aegean, Karlovassi, Samos, Greece

Keywords: Information Security Management, Privacy, Human Behaviour.

Abstract: Why do people who claim to be concerned about privacy disclose their personal information on social media? Why do users that are aware of security threats often neglect to take protective measures? Why do loyal employees sometimes fail to comply with security policies? Why do infosec managers often insist on practices and policies that have been proven to be ineffective? These and several more questions arise whenever we observe individuals’ security and privacy behavior and despite the vast amount of research in the field, we still lack a comprehensive explanation.

In this talk, we’ll explore privacy and security behavior from multiple perspectives, including cognitive biases and decision-making heuristics, latent incentives, socio-cultural dispositions, and organizational politics. We’ll show that no single theoretical model can provide sufficient guidance and, thus, it is important to adopt a multidisciplinary and multi-theoretical approach.

1 INTRODUCTION

Why do people who claim to be concerned about their privacy disclose their personal information on social media? Why do users that are aware of security threats often neglect to take protective measures? Why do loyal employees sometimes fail to comply with security policies? Why do infosec managers often insist on practices and policies that have been proven to be ineffective? These questions arise when we observe individuals’ actual security and privacy behaviour. Unfortunately, there are no concrete and comprehensive answers yet. Nevertheless, researchers have been investigating the factors that determine human security and privacy behaviour and have provided some interesting results.

In the following paragraphs, we shall present some key privacy and security behaviour issues and provide insight into the psychological, political, and social aspects of these issues.

2 INEFFECTIVE INFORMATION SECURITY PRACTICES

Research on information security behaviour has focused on the insecure practices that users often follow and users’ noncompliance with information security policies and guidelines. Nevertheless, it’s not only common users that follow insecure practices. Information security managers and experts often adopt ineffective strategies, although they are well trained and capable of identifying these inefficiencies. Some examples follow.

- Chief Information Security Officers (CISOs) often insist on password policies that require frequent password changes, although this practice is obsolete (NIST, 2017).
- CISOs publish lengthy policies written in an obscure language and send lengthy email notifications and guidelines.
- Top management executives often fail to enforce information security policies, although they understand their importance.

The National Institute of Standards and Technology (NIST) has published guidelines (NIST, 2017) that require organizations not to impose periodical password changes. NIST SP 800-63B states that “[v]erifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator”. Most information security experts also agree that frequent password changes, as well as complex password composition rules are ineffective.

Kokolakis, S.
Security, Privacy and the “Human Factor”: Making Sense of the Paradoxes of Security and Privacy Behaviour.
DOI: 10.5220/0012640600003648

In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 9-11
ISBN: 978-989-758-683-5; ISSN: 2184-4356

For example, a user may adopt the following monthly password change practice that complies with strict policies, but it is obviously insecure:

- January: P1a1s1s1@
- February: P2a2s2s2@
- March: P3a3s3s3@
- April: P4a4s4s4@
- …

Although most CISOs are aware of the above, they may retain ineffective policies for reasons that are more "political" rather than scientific. They might be afraid of "passing the wrong message that we relax our security requirements" or getting blamed in case of compromise.

The relation between business politics and information systems' use and management has been studied since the early '80s (Markus, 1983). The field of information security management could also benefit from an interdisciplinary approach that takes into account the political and power aspects of information security decision making and behaviour.

The political and power-related perspective could also illuminate the adoption of similarly ineffective practices, such as publishing complex policies and lengthy notifications. CISOs may develop several policies that span hundreds of pages and send lengthy emails to employees, although they know that few people will actually read them. This paradoxical behaviour could be explained, if we examine how executives in an organization deal with responsibility. In this case, CISOs may aim to make sure that the responsibility for compliance lies with users.

Understanding business politics and power balances in organizations could also shed light on top management's attitude towards information security. Although top management may acknowledge the importance of information security, they could be reluctant to enforce policies that require a large amount of "political capital" to be spend.

The information systems research community has used various frameworks to study socio-technical issues, such as the above. A socio-technical framework that applies to information security management is Actor-Network Theory (Latour, 2007; Tsohou et al., 2015).

Actor-Network Theory (ANT) provides a theoretical framework for studying how networks of actors are formed to achieve agreed objectives. ANT considers both human and non-human (i.e., technological) actors that enroll in a network with a specific objective. In previous research, Tsohou et al. (2015) have applied ANT to show how information security executives can achieve the effective implementation of an information security awareness programme.

Concluding, we may note that information security behaviour depends on a complex system of motives, interests, alliances, and conflicts. Accordingly, we should enhance our theoretical models to account for the social, political and power-related aspects of information security practice.

3 THE PRIVACY PARADOX

The term *privacy paradox* has been used to refer to situations where people although they state that they value their privacy, they disclose their personal information for very small rewards (Kokolakis, 2017). Addressing the privacy paradox requires a study of human psychology and behaviour. Several researchers have focused on how people make decisions concerning information disclosure (Acquisti et al., 2015). They noted that human decision making is biased and, thus, people often fail to make decisions that are optimal and in alignment with their values and objectives. Some of the biases that influence privacy decision making are the following:

Optimism Bias. People systematically tend to believe that others are at higher risk to experience a negative event compared to themselves (Baek et al., 2014). As a result, people are immune to fear appeals. They understand the risks, but they are still optimistic that "it won't happen to them".

Affect Heuristic. The affect heuristic refers to a cognitive shortcut, in which current emotion influences judgements and decisions. Privacy-related decisions are hard to predict, they may depend on the moment's emotion.

Hyperbolic Time Discounting. Hyperbolic time discounting refers to the common tendency to attribute greater importance to present gains or losses than to future ones. The consequences of information disclosure might come sometime in the future. Thus, the immediate gratification of sharing information may outweigh future privacy risks.

If we assume that personal information disclosure decisions are based on a calculation of the expected loss of privacy and the potential gains of disclosure, then we should expect that the above biases would affect these calculations. Optimism bias would lead to an undervaluation of expected loss of privacy, since people tend to be optimistic that a privacy violation would not affect them.

Also, due to hyperbolic time discounting, individuals would underestimate future consequences of personal information disclosure. Finally, the above calculations would be affected by the emotional status of the individuals the moment they make their decision to disclose or not. Thus, we should not expect them to be consistent in their decisions.

Moreover, there are strong motivations for self-disclosure, especially in the social media. Self-disclosure is an important element in building relations and gaining acknowledgement in social networks. Social network users invest in social capital, i.e. the value derived from positive connections with other people. They create bonds with other network members anticipating that they will receive their support when needed.

Privacy behaviour that contradicts stated privacy values seems to be “irrational”. Nevertheless, human thinking is very complex and viewing it through the lenses of the rational vs. irrational dualism is oversimplistic. Kahneman (2011) distinguishes two “systems of thinking”:

- System 1: Fast, intuitive, based on experience, “automatic”.
- System 2: Analytical, “reasonable”.

The two systems work in tandem and cannot be separated. Although we are only aware of System 2 thinking, both systems are equal and no system has precedence over the other. Human behaviour often seems irrational, but that’s only because we tend to ignore or undervalue System 1.

System 1 uses heuristics, rather than an analytical assessment process and it is fast, versatile, and adaptable. However, a side-effect of humans’ versatility and adaptability is that they are not consistent in their behaviour.

System 2 also has limitations. Most people are lacking the cognitive ability to calculate potential gains and losses. There are numerous parameters to consider, whilst the computational capacity of humans is limited and they cannot perform complex calculations. Individuals also lack the necessary information to make accurate calculations. Usually, they can only guess how their personal information will be treated.

Information asymmetries are dominant in the relationship between data consumers and data providers. Individuals have very little knowledge of how their personal data are used and privacy policies are too complex for them to understand.

4 CONCLUSIONS

Human behaviour often seems paradoxical or irrational, especially with respect to information security and privacy. Research models may approach different aspects of information security and privacy behaviour, but no model is ever strong enough to cover all aspects of human behaviour.

Researchers that aim to investigate security and privacy behaviour have no other option but to adapt an interdisciplinary approach. The social, cognitive, and psychological dimensions are pervasive and most important when studying these issues.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, **347**(6221), 509-514.

Baek, Y. M., Kim, E. M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, **31**, 48-56.

Kahneman, D. (2011). *Thinking, fast and slow*. Macmillan Publ.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, **64**, 122-134.

Latour, B. (2007). *Reassembling the social: An introduction to actor-network-theory*. Oxford.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, **24**(1), 38-58.

NIST (2017). Digital Identity Guidelines: Authentication and Lifecycle Management. *National Institute of Standards and Technology SP 800-63B* Available at: https://doi.org/10.6028/NIST.SP.800-63b.