Personal and Ubiquitous Computing (2021) 25:809–812
https://doi.org/10.1007/s00779-021-01591-8

EDITORIAL

The current state of research on people, culture and cybersecurity

Jongkil Jay Jeong[1] · Gillian Oliver[2] · Eunsuk Kang[3] · Sadie Creese[4] · Peter Thomas[5]

Published online: 30 June 2021

1 Introduction

There are an ever-increasing number of cybersecurity-related incidents reported worldwide despite increased spending on cybersecurity. It seems that improved algorithms, systems and processes alone are not able to keep digital systems secure. What is becoming apparent is that we need a better understanding of the human aspects of cybersecurity not only in terms of its impacts on organisations, communities and individuals but also in terms of how human behaviour itself contributes to cybersecurity-related incidents. This is a challenge. A cohesive understanding of the human aspects of cybersecurity is only possible through an interdisciplinary approach that includes both behavioural and social sciences alongside information technology and computer security.

Therefore, the aim of this special issue is to contribute to our understanding of the social and cultural factors of cybersecurity by bringing together research from unique and diverse disciplinary backgrounds to which will enable us to broaden and deepen understanding of the dimensions of cybersecurity and provide the foundation for effective strategies.

✉ Jongkil Jay Jeong
jay.jeong@deakin.edu.au

Gillian Oliver
Gillian.Oliver@monash.edu

Eunsuk Kang
eunsukk@andrew.cmu.edu

Sadie Creese
sadie.creese@cs.ox.ac.uk

Peter Thomas
peter.thomas@haileybury.vic.edu.au

[1] Centre for Cyber Security Research and Innovation, Deakin University, Geelong, Australia

[2] Monash University, Melbourne, Australia

[3] Carnegie Mellon University, Pittsburgh, USA

[4] Oxford University, Oxford, UK

[5] HaileyburyX, Melbourne, Australia

2 Summary of accepted papers

Nine articles were selected for this special issue from 25 submissions. They cover topics ranging from exploring privacy and security issues from an individual perspective to examining national cybersecurity capacity building through a socio-cultural lens across a wide range of disciplines including media and communication studies, linguistics, sociology, psychology, information and computer sciences as well as education.

The nature of the studies was also as diverse as the disciplinary areas identified, with a mixture of application-oriented, theoretical, technological, methodological and survey-based studies. We briefly introduce each of the articles below.

2.1 Study [1]: the importance of social identity on password formulations

This study examines how socio-cultural factors play a formative role in determining the relative strength of passwords set by the general public. Through an analysis of 1.3 billion username/password combinations, the results from their study suggest that users' behaviour towards passwords differs between countries, with the social identity of a user playing a definite role in how passwords are generated.

More importantly, findings suggest that poor password formulation behaviours are globally inherited and that despite the popularity of passwords as a means for authenticating credentials, they remain highly vulnerable to simple attacks, such as dictionary attacks, and can therefore not be regarded as an overly trusted authentication mechanism. As a means to address this issue, authors recommend additional means of authentication such as multi-factor authentication or

implementing a single sign on federated login service which will enable users to establish stronger password practices.

2.2 Study [2]: from awareness to influence: towards a model for improving employee security behaviour

This paper focuses on an in-depth case study of a leading Australian telecommunications company to examine how to imitate change in the approach of employees towards security behaviours from awareness to influence. The study adopts Kelman's psychological attachment theory to argue that most employees *comply* with company policy as long as they are being monitored and assessed.

Their study argues that this inherent behaviour towards compliance is a temporary and superficial one and describes how the addition of a cybersecurity champion who influenced others on the importance of cybersecurity, established key relationships with stakeholders and built trust with employees from multiple areas of the business enabled the business to evolve from just a compliance level, to one where employees follow security policies because they have the same beliefs and value system with the cybersecurity team thus enabling meaningful behavioural change.

2.3 Study [3]: the stray sheep of cyberspace a.k.a. the actors who claim they break the law for the greater good

This study examines a typology of hackers — hacktivists; cybermilitia members and Internet trolls and their motivation behind using the Internet for malicious purposes. The study argues that, in contrast to the traditional motives of a hacker which is to engage in computer-related offences of various significance and impact such as trying to exploit systems' vulnerabilities, disseminate malicious software and steal data or funds, the internal motivation of these hacker groups are not always utterly sinister; actually, some of them firmly believe that their actions are for the greater good.

The authors argue that these subgroups of hackers who are not driven by malicious intent present difficult situations for law enforcement and policy as well as create ethical dilemmas pertaining to whether their actions merely represent a means for them to communicate their ideology or sentiment or if the law is law and they should be punished irrespective of their intent and motives.

2.4 Study [4]: case-based learning in the management practice of information security: an innovative pedagogical instrument

This study examines how case-based learning (CBL) approaches can improve the quality of education provided on matters pertaining to information security (IS). The authors develop, refine and evaluate a teaching case of a hypothetical firm that suffers a catastrophic incident of intellectual property (IP) theft with post-graduate students from the University of Melbourne, Australia.

Through survey data collected across two consecutive years from the students pertaining to CBL, their results suggest that students strongly agreed that the teaching case was relevant, realistic, engaging, challenging and instructional. Based on these outcomes, they developed a pedagogical instrument that can be used by both academics and industry to design courses to educate not only students but also executives and managers on the importance of effective information security management practices.

2.5 Study [5]: I'm all ears! Listening to software developers on putting GDPR principles into software development practice

This study highlights the challenges developers face when incorporating privacy-preserving principles based on the General Data Protection Regulation (GDPR) when developing software applications.

Based on interviews with 22 developers, the authors identified several issues pertaining to the challenges developers face when embedding privacy-preserving GDPR principles. These issues generally spanned across the lack of knowledge of GDPR in general, thereby resulting in a lack of understanding of the techniques and necessary resources to take into consideration. Furthermore, developers were more focused on the functional aspects, and ensuring that the goals and objectives of the various stakeholders were addressed first.

2.6 Study [6]: understanding users' perceptions to improve fallback authentication

This study examines the feasibility of security questions as a means for fallback authentication. Based on a multi-phase qualitative study involving 30 participants, they explored how users select security questions, what strategies are used to memorise answers, how users perceive the security and memorability of their answers and how a technique which addresses key security weaknesses (but makes them less memorable) impacts users' perceptions.

Results from the study revealed that despite asking participants to select security questions for an online banking scenario, participants who answered security questions with their own answers did not consider security factors. Instead, they selected easy, truthful and certain answers. Memorisation strategies were ignored by most participants (even those who used unfamiliar answers). To mitigate some of these issues, the paper provides recommendations pertaining to improving the design of the security questions.

2.7 Study [7]: the role of self-efficacy on the adoption of information systems security innovations: a meta-analysis assessment

This study examines the role of self-efficacy through a meta-analysis and subsequent synthesis of 59 extant research publications. The findings suggest that individuals with stronger self-confidence for tackling IS security threats are more likely to adopt IS security innovation.

Through a meta-analysis moderator effect examination, the study further demonstrates that some research conditions may influence the outcome of the relationship between self-efficacy and the adoption of IS security innovations. The conclusion is that those who are in charge of IS security management in organisations should target increasing employee's self-efficacy.

2.8 Study [8]: a framework and tool for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture

This study proposes a framework which addresses the issues pertaining to building a culture which demonstrates secure behaviour amongst staff members with minimal resources. Their focus was specifically on information technology (IT) staff members, as they argued that they play an integral part of supporting and sustaining the key technologies that are incorporated by an organisation.

An evaluation tool to assess and apply the framework is also developed, which takes into consideration the measurement of assessment, cost reduction and sustainability aspects pertaining to information security. The subsequent framework and assessment tool was to highlight its strengths, weaknesses and opportunities through an expert review process.

2.9 Study [9]: the social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions

Through a study of the social and cultural aspects of cybersecurity capacity building across 78 nations, the authors found evidence to suggest that regional differences exist even amongst countries that are expected to share similar attitudes, values and practices around cybersecurity due to cross-national differences in development and the scale of Internet use.

The findings from this study suggest that the national development of cybersecurity is separate from the existing social and cultural frameworks established at a national level and therefore the values, attitudes and practices amongst Internet users within nations are based on a separate *cybersecurity culture*.

3 Emerging trends and future directions

The research papers accepted for this special track re-emphasise the fact that whilst cybersecurity in its core essence is indeed a technical issue, the concerns that arise from this challenge impact us from a range of technical and non-technical levels. Although a wide range of different subjects, methodologies and disciplinary areas were identified from the accepted papers, a synthesis of the studies presented in "Section 2" highlighted three major trends emerging from the studies on people, culture and cybersecurity based on this special theme issue.

Firstly, there were a number of studies which examined cybersecurity from the unit of analysis perspective of the *individual level*. Considering that nearly half of all cybersecurity incidents are due to human errors [10], the focus on individuals and how they make decisions and what influences them within digital environments is timely research subject matter. Secondly, a trend towards *qualitative case studies* examining socio-cultural factors and their impact on cybersecurity was also identified amongst the studies as well. Socio-cultural and human factors in cybersecurity is still an under-explored topic, and qualitative studies such as the ones accepted for this special issue will help shed light on the different contexts and nuances that surround cybersecurity. Finally, there was a significant focus on *cybersecurity education and awareness*, and how this can be enhanced at both an organisational and national level. Recent studies have highlighted the correlation between the level of education and training received and the boost towards situation awareness and cybersecurity in general [11], and several studies from this special issue also demonstrated similar outcomes and results.

The primary aim of the special issue was to identify and share novel research studies which enrich our understanding of people, culture and cybersecurity. In this regard, we hope that the literature covered in this editorial will provide future studies a reference point when examining the socio-cultural and human factors pertaining to cybersecurity.

Acknowledgements We thank the authors who have contributed through submitting their papers, along with the editors and reviewers for providing their time and expertise towards this special issue.

References

1. Grobler M, Chamikara M, Abbott J, Jeong JJ, Nepal S, Paris C (2020) The importance of social identity on password formulations. Pers Ubiquit Comput:1–15
2. Alshaikh M, Adamson B (2021) From awareness to influence: toward a model for improving employees' security behaviour. Pers Ubiquit Comput:1–13
3. Pawlicka A, Chorás M, Pawlicki M (2021) The stray sheep of cyberspace aka the actors who claim they break the law for the greater good. Pers Ubiquit Comput:1–10

4. Ahmad A, Maynard SB, Motahhir S, Anderson A (2021) Case-based learning in the management practice of information security: an innovative pedagogical instrument. Pers Ubiquit Comput:1–25
5. Alhazmi A, Arachchilage NAG (2021) I'm all ears! listening to software developers on putting GDPR principles into software development practice. Pers Ubiquit Comput:1–14
6. Micallef N, Arachchilage NAG (2021) Understanding users' perceptions to improve fallback authentication. Pers Ubiquit Comput: 1–33
7. Hameed MA, Arachchilage NAG (2021) The role of self-efficacy on the adoption of information systems security innovations: a meta-analysis assessment. Pers Ubiquit Comput:1–15
8. Govender S, Kritzinger E, Loock M (2021) A framework and tool for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture. *Pers Ubiquit Comput*:1–14
9. Creese S, Dutton WH, Esteve-González P (2021) The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. Pers Ubiquit Comput:1–15
10. J. Jeong, J. Mihelcic, G. Oliver, and C. Rudolph (2019) "Towards an improved understanding of human factors in cybersecurity," in 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), pp. 338–345.
11. Öğütçü G, Testik ÖM, Chouseinoglou O (2016) Analysis of personal information security behavior and awareness. Computers & Security 56:83–93