Cybersecurity Behaviour: A Conceptual Taxonomy

Thulani Mashiane, Elmarie Kritzinger

Cybersecurity Behaviour: A Conceptual Taxonomy

Thulani Mashiane[1] and Elmarie Kritzinger[1]

School of Computing,University of South Africa, PO Box 392, UNISA, 003, South Africa

Abstract. User cybersecurity behaviour is a concern for organisations as well as home users. This is because cyber-criminals have made a shift from targeting security systems to targeting the users of the systems. As a result, an increasing number of studies have been conducted in efforts to understand user cybersecurity behaviour. The advantage in understanding user behaviour is that researchers and security practitioners can apply this knowledge and begin to change behaviour to benefit cybersecurity. Different studies have categorised similar cybersecurity behaviours, however the naming conventions differ across studies. This brings out the first contribution of the paper, unified terminology for the cybersecurity behaviour. Secondly, most studies were conducted in an organisational setting. User behaviour in other environments is yet to be identified and categorised. The second contribution of this study is the identification and categorisation of home user cybersecurity behaviour. The identification and classification of more cybersecurity behaviour is aimed to have a positive impact in the creation of strategic interventions to change and maintain good cybersecurity behaviour.

Keywords: Cybersecurity behaviour· Classification, Taxonomy· Cybersecurity.

1 Introduction

To decrease the number of cyber incidents, it is key that users, especially user behaviours, are understood to understand how to change user behaviour. An initial step is the identification and classification of user cybersecurity behaviour.

1.1 Cybersecurity Behaviour (CSB)

Human behaviour refers to an individual's actions, reactions, mannerisms and conduct within different environments [4]. Cybersecurity behaviour (CSB) is therefore defined, by the current research, as an individual's actions, reactions, mannerisms, and general conduct in the cyber domain. The goal of studying user CSB is to promote good CSB while decreasing malicious or bad CSB.

1.2 Cybersecurity Behaviour Context

Researchers [5, 6] have noted that users act differently in different settings. But, the categorisation of CSB has been focused mainly on behaviour in organisations. Numerous targets of cybersecurity attacks fall outside the context of the organisation [7]. Therefore, a gap exists in literature, where other cybersecurity contexts have been left out. The importance of including different contexts is the ability to accurately categories CSB.

1.3 Cybersecurity Behaviour Taxonomy

To understand a system, it is necessary to understand the components that make up that system. A taxonomy is a tool used to classify components in a domain. Making use of a taxonomy allows for the structural organisation of concepts that make up the system. CSB have been expressed in the form of taxonomies. More recently, Bitton et al. presented a taxonomy for mobile cybersecurity awareness [8]. The current study builds on previously published taxonomies in the classification of users' CSB.

The remainder of the paper is presented as follows. Section 2 presents a literature review and Section 3 presents the proposed conceptual taxonomy. The conclusion and future work is presented in Section 4.

2 Literature Review

The following section presents literature that focuses on user CSB in the workplace as well as at home.

2.1 Cybersecurity Behaviour

Context is made up of the circumstances surrounding a behaviour. Context has an influence on behaviour [10]. An example related to CSB is: social engineering attacks may be more effective at certain times of the year, such as the festive season. In this section, the CSB in the work and home context are discussed.

Cybersecurity Behaviour at Work The CSB of employees is mostly governed by policies and regulations. Employees are held accountable for misconduct or not adhering to the organisational rules [11, 12]. Furthermore, ICT departments assist users in adhering to policy by sending reminders about software updates, information on new threats, information best practices, and blocking dangerous or inappropriate sites [9].

Blythe strived to understand CSB in an organisational setting [13]. In an organisational setting, cybersecurity is usually evaluated as a function of compliance [14]. In an organisation, bad CSB is seen as noncompliance to the set policies. Blythe contended that behaviour is more entailed than this. The study argued that the evaluation of compliance is limited in that it tests a small scope of policies and procedures. Among other behavioural determinants, the behaviour

is a function of interior and exterior influences. Interior influences include self-motivation or drive, similar to intentions mentioned in [9], while exterior influences are features such as the environment [13].

To categorise CSB in organisations, a six-element taxonomy was developed by Stanton et al. The dependent variables used to group the behaviours were 1) the amount of expertise required to carry out the behaviour, and 2) the intention towards the organisation when carrying out the behaviour. The six categories of the taxonomy where: *intentional destruction, dangerous tinkering, aware assurance, detrimental misuse, nave mistakes,* and *basic hygiene* [9].

Intentional destruction, detrimental misuse, dangerous tinkering, and nave mistakes are examples of bad CSB and aware assurance and basic hygiene are examples of good CSB. To visualise the taxonomy, the categories of the taxonomy were put on a two-dimensional plane. On the x-axis, the intention of the user is plotted; intentions range from malicious to unintentional. On the y-axis, the user expertise ranging from expert to novice are plotted (see Fig. 1.).

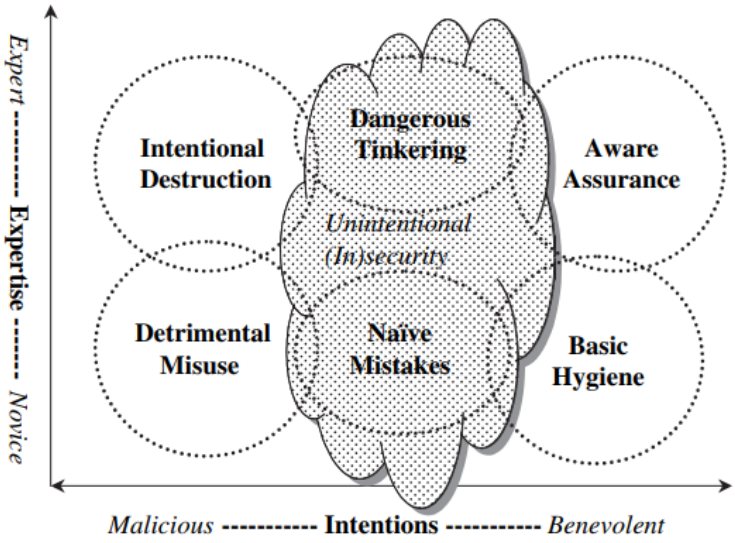

Fig. 1. End User Security Behaviours [9]

Taking and expanding on the work by Stanton et al., Djajadikerta et al. made use of the four classifications (Intentional Destruction, Dangerous Tinkering, Detrimental Misuse and Nave Mistakes) to further investigate bad information security behaviour [16]. The four classifications were verified by placing organisational CSB concerns into each group.

Guo observed the disparities in the conclusions of information systems behaviour research. The different, often contradicting results were hypothesised to be due to methodological issues or the ill definition of information system's

behaviour. The study realised the need for more clear definitions of information systems behaviours. Through the review and synthesis of previous studies, a conceptual framework was designed which incorporates four categorisations of organisational behaviour: *security assurance behaviour, security compliant behaviour, security risk-taking behaviour,* and *security damaging behaviour* [17].

Chu, Chau, and So developed a typo-logical theory for information security deviant behaviour in an organisational setting [18]. The result of the study categorised cybersecurity into four categories: *Misuse of information systems resources, Information security carelessness, System protection deviance* and *Access control deviance.*

In terms of CSB at work, Fig. 2 presents a graph with the cybersecurity categories taken from the studies presented in Section 2. The categories are plotted on the same graph that was used in the research by Stanton et al. [9].

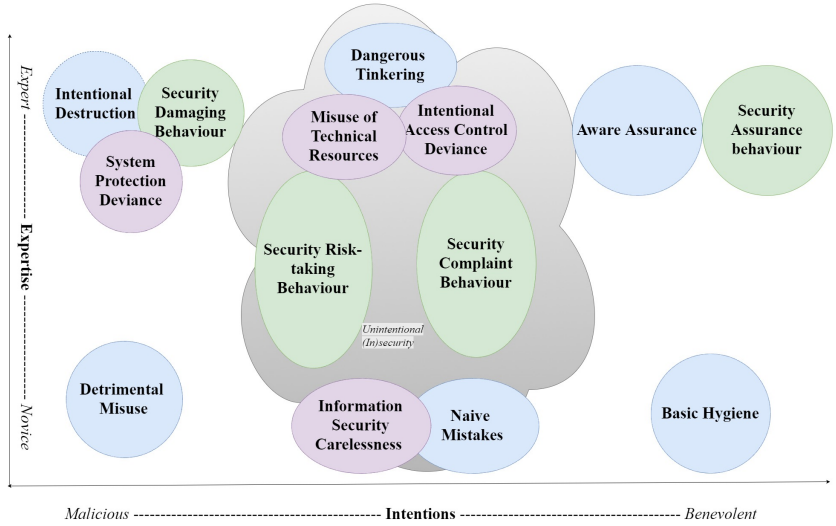

Fig. 2. Cybersecurity Behaviour in Organisations [9, 17, 18].

The graph shows most of the categories identified require some level of cybersecurity expertise. This implies that users in organisations, generally, have the expertise in cybersecurity. An inference can be made that CSB in organisations is not hindered by the lack of cybersecurity expertise.

The next important observation is that a majority of the security behaviour categories are not intended on malicious or benevolent behaviour. This neutral attitude towards cybersecurity is a risk because users, then show no interest in improving or applying their skills.

Currently, through the graph in Fig. 2, it is not clear what the intentional difference between Security Risk taking behaviour and Security Compliance behaviour is. It is therefore a need that a clear distinction in intentions is derived. This distinction must also be represented, though the graph.

Cybersecurity Behaviour at Home

Home users are individuals of different ages that make use of computers or mobile devices that connect to the Internet. In the home context, users are typically solely responsible for managing their CSB. It is assumed that cybersecurity knowledge, awareness and skills are much lower for home users, as they are not exposed to training programs [19]. This assumption was later proven false by [20] where it was found that home users do have cybersecurity knowledge and skills. The knowledge may be gained from other environments such as work, but the behaviour at home is different [11, 21].

Lastly, there are home users that do follow cybersecurity principals at home. Cybercitizens is a term found in the study by Catherine et al. Cybercitizens describe home users that are proactive in being cybersecurity aware and applying cybersecurity skills in their environments [19]. The study focuses on the intentions of cybercitizens and presents interventions to encourage more users to become cybercitizens. The type of behaviours that a cybercitizen exhibits are installing and updating antivirus software, be cautious of emails as well as email attachments, and lastly choosing strong and easy to remember passwords [19].

3 Proposed Conceptual Cybersecurity Behaviour Taxonomies

The proposed CSB taxonomy addresses the two points: 1) Ambiguity in cybersecurity intentions, and 2) Completeness in the introducing of context as an independent variable when categorising CSB.

3.1 Updated Work Cybersecurity Behaviour Taxonomy

The current section proposes an updates CSB taxonomy for the work environment. The contribution in this section is the division of behaviour intentions into four categories.

Fig 3 presents the CSBs at work with the derived intentions. This new graph offers the advantage of clearly showing the intentions associated with the categories of behaviours. headings should be numbered. Lower level headings remain unnumbered; they are formatted as run-in headings.

Intentions

Intentions are plans for performing a behaviour. The literature on CSB intentions can be divided into intentional and unintentional CSB [25].

Intentional Cybersecurity Behaviour Intentional CSB refers to instances where the user purposefully wants to harm systems or disregard cybersecurity principals. Opposite to this, users can purposefully uphold or/and promote cybersecurity principals.

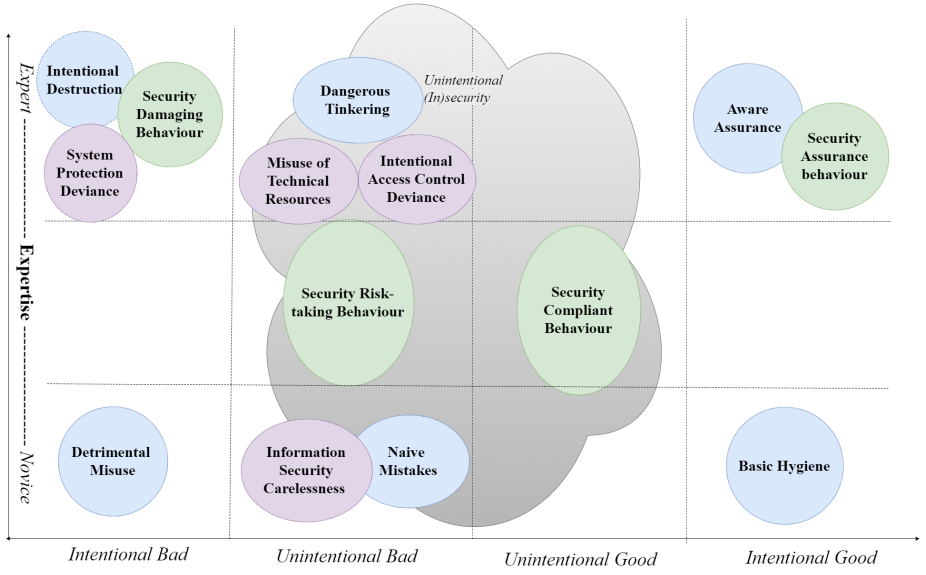

Fig. 3. Work CS Behaviour with Segmented Intentions adapted from [9, 17, 18].

Intentional Bad (IB) Cybersecurity Behaviour This category of users shows dysfunctional CSB. The categorisation is adapted from research done by Stanton et al. were categories such as intentional destruction and detrimental misuse where used to describe users' dysfunctional CSB [9, 16]. Users that show this type of harmful CSB are called cybercriminals, hackers, crackers and script kiddies. Examples of behaviour include website defacement, spamming, unauthorised system access, malware and malware distribution and vulnerability exploitation.

Intentional Good (IG) Cybersecurity Behaviour There exist instances where the user purposefully upholds cybersecurity principles [9]. This category is adopted from Stanton et al. where aware assurance and basic hygiene are collapsed into intentional good CSB. An example of users performing intentional good CSB are users that create good passwords to protect information belonging to them or an organisation. Literature has developed terms such as good cybersecurity hygiene and conscious care behaviour to describe this category of users [9, 26].

Unintentional Cybersecurity Behaviour Unintentional CSB refers to instances where the user does not intend on disregarding nor upholding cybersecurity principals. In these instances, good or bad CSB is a by-product of other actions or intentions.

Unintentional Bad (UB) Cybersecurity Behaviour Behaviours categorised as unintentional bad CSB are those where the user does not intend to cause malicious harm or purposefully disregard cybersecurity principals. Ifinedo referred to these behaviours as counterproductive computer security behaviours [27], while

Stanton et al. referred to it as dangerous tinkering and nave mistakes [9] and Chu et al. refers to it as information security deviant behaviour [18]. An example of unintentional bad CSB is a user that writes their password down or recycles their password [28].

Unintentional Good (UG) Cybersecurity Behaviour Behaviours categorised as unintentional good CSB are behaviours where users preserve cybersecurity because of other intentions or actions. The study by Virginia Tech found that even though users complied with password change policies, the users still felt that cybersecurity is an obstacle. In this case, the intention of the behaviour is to comply, and it is not to practice good CSB [29]. Unintentional good CSB is not ideal, because for a behaviour to be repeated the user must be intentional in repeating as well as sustaining the behaviour.

3.2 Home Cybersecurity behaviour Taxonomy

Categories captured in Fig. 3's graph focus on CSB that occur at work. In the interest of completeness, the next section of the study aims to categorise CSBs of home users. To do so, different CSBs were extracted from literate. These behaviours were plotted on a similar graph as used in Fig. 4. However, the y-axis had to be adjusted. According to the literature presented, home users do have cybersecurity knowledge and skills. In the home environment the application of these knowledge and skills is more distinguishing of the behaviours as opposed to having the knowledge and skills. Therefore, the y-axis is divided into *None or Limited Knowledge and Skills, Knowledge and Skills but No Implementation* and finally*, Knowledge and Skills with Implementation.*

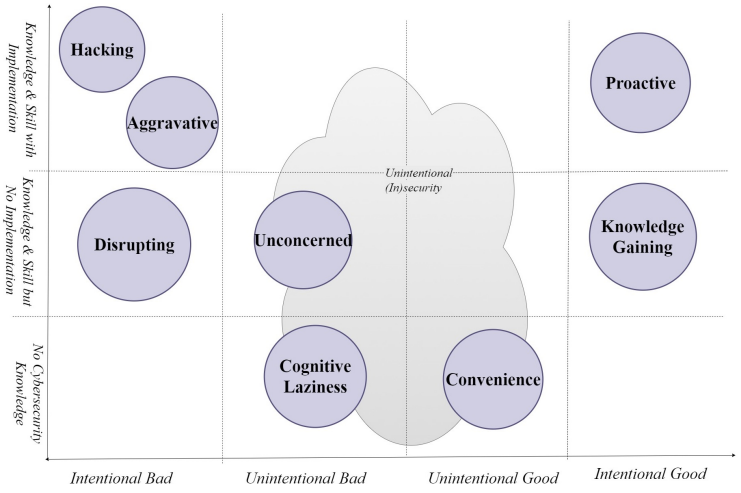

Fig. 4. Home Users'Cybersecurity Behaviour Categories

Eight CSB categories were derived for the home user behaviour taxonomy: *Hacking, Aggravative, Disrupting, Unconcerned, Cognitive Laziness, Convenience, Proactive* and *Knowledge Gaining*. The categories are a result of plotting 95 CSBs on a graph similar to Fig. 4. CSB plotted close together were then grouped together to form the resulting graph in Fig. 4.

In Fig 4 in the Knowledge and Skills with Implementation there are three behaviour categories, namely Hacking, Aggravating and Proactive. Hacking and Aggravating behaviours are intentional bad behaviours, while Proactive is intentional good behaviour. Hacking are behaviours that seek out to cause harm to other systems and people though technical expertise, while aggravate behaviours are targeted at other people especially on social media sites.

In the Knowledge and Skills with no Implementation there are three behaviour categories, namely Disrupting, Unconcerned and Knowledge Gaining. Disrupting behaviours are intentional bad CSBs. The behaviours under this category show neglecting of cybersecurity principals through the reckless actions such as downloading torrents from peer-to-peer networks. The category Unconcerned describes careless CSBs. However, the intention of these behaviours in not to intentionally cause harm. Knowledge gaining CSB is intentionally good behaviour. However, without applying the knowledge and skills these behaviours have little use in maintaining cybersecurity.

In the No or Limited Knowledge row there are two behaviour categories, namely Cognitive Laziness and Convenience. These terms were taken from [30]. Cognitive Laziness is unintentional bad CSB. This category of behaviours describes behaviour that is done mindlessly without consideration of any cybersecurity. Finally, the Convenience category describes unintentional good CSB. These behaviours are done only if the cybersecurity related task is convenient.

4 Conclusion

The aim of the paper was to provide a clear representation and visualisation of CSB. The study reviewed literature on CSB in the workplace. The literature was consolidated and represented on one graph. Previous research had represented user intentions of CSB on an ordinal scale ranging from malicious to benevolent. The current study improved on this measurement by dividing intentions into smaller units of measurement. The result was four categories to describe user CSB intentions. The second half of the paper focused on home user CSB. Eight categories of home user CSB were presented. The categories were obtained by plotting home user CSB found in literature against knowledge and skill implementation and user intentions. The information in this study contributes to the understanding of user CSB and can be used by researchers and practitioners of cybersecurity. This research aids in specifying the question from How to change CSB? to How to change CSB of home users who exhibit *Cognitive Laziness* behaviour. Future work will need to conduct an experiment to verify the conclusions found in this study. Future work will also need to address the influences of CSBs.

References

1. Abrams, M. and J. Weiss, Malicious control system cyber security attack case studyMaroochy Water Services, Australia. McLean, VA: The MITRE Corporation, 2008.
2. Smith, S.N., et al., The Impact of Monetary Value Gains and Losses on Cybersecurity Behavior. 2017.
3. Anwar, M., et al., Gender difference and employees'cybersecurity behaviors. Computers in Human Behavior, 2017. 69: p. 437-443.
4. Scheflen, A.E., How behavior means. 1973: Gordon and Breach New York.
5. Liang, H. and Y. Xue, Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 2010. 11(7): p. 394-413.
6. Kruger, H.A., et al. An assessment of the role of cultural factors in information security awareness. in Information Security South Africa (ISSA), 2011. 2011. IEEE.
7. Bjrnhaug, T., Internet of Things-Cybersecurity at Home, 2017, NTNU.
8. Bitton, R., et al., Taxonomy of mobile users'security awareness. Computers & Security, 2018. 73: p. 266-293.
9. Stanton, J.M., et al., Analysis of end user security behaviors. Computers & security, 2005. 24(2): p. 124-133.
10. Acquisti, A., L. Brandimarte, and G. Loewenstein, Privacy and human behavior in the age of information. Science, 2015. 347(6221): p. 509-514.
11. Kritzinger, E. and S.H. von Solms, Cyber security for home users: A new way of protection through awareness enforcement. Computers Security, 2010. 29(8): p. 840-847.
12. Safa, N.S., R. Von Solms, and S. Furnell, Information security policy compliance model in organizations. Computers Security, 2016. 56: p. 70-82.
13. Blythe, J., Cyber security in the workplace: Understanding and promoting behaviour change. Proceedings of CHItaly 2013 Doctoral Consortium, 2013. 1065: p. 92-101.
14. Bulgurcu, B., H. Cavusoglu, and I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 2010. 34(3): p. 523-548.
15. Deibert, R.J. and R. Rohozinski, Risking security: Policies and paradoxes of cyberspace security. International Political Sociology, 2010. 4(1): p. 15-32.
16. Djajadikerta, H.G., S.M. Roni, and T. Trireksani, Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research. Information Management, 2015. 52(8): p. 1012-1024.
17. Guo, K.H., Security-related behavior in using information systems in the workplace: A review and synthesis. Computers Security, 2013. 32: p. 242-251.
18. Chu, A.M., P.Y. Chau, and M.K. So, Developing a Typological Theory Using a Quantitative Approach: A Case of Information Security Deviant Behavior. CAIS, 2015. 37: p. 25.
19. Anderson, C.L. and R. Agarwal, Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS quarterly, 2010. 34(3): p. 613-643.
20. Edwards, K., Examining the security awareness, information privacy, and the security behaviors of home computer users. 2015.

21. Talib, S., N.L. Clarke, and S.M. Furnell. An analysis of information security awareness within home and work environments. in Availability, Reliability, and Security, 2010. ARES'10 International Conference on. 2010. IEEE.
22. Li, Y. and M.T. Siponen. A Call For Research On Home Users'Information Security Behaviour. in PACIS. 2011.
23. Sharma, K., Impact of framing and priming on users'behavior in cybersecurity. 2017.
24. Bada, M. and A. Sasse, Cyber Security Awareness Campaigns: Why do they fail to change behaviour? 2014.
25. Safa, N.S., R. Von Solms, and L. Futcher, Human aspects of information security in organisations. Computer Fraud Security, 2016. 2016(2): p. 15-18.
26. Safa, N.S., et al., Information security conscious care behaviour formation in organizations. Computers Security, 2015. 53: p. 65-78.
27. Ifinedo, P. Effects of Organizational Citizenship Behavior and Social Cognitive Factors on Employees'Non-Malicious Counterproductive Computer Security Behaviors: An Empirical Analysis. in CONF-IRM. 2015.
28. Nthala, N. and I. Flechais. If Its Urgent or It Is Stopping Me from Doing Something, Then I Might Just Go Straight at It: A Study into Home Data Security Decisions. in International Conference on Human Aspects of Information Security, Privacy, and Trust. 2017. Springer.
29. Tech, V., When users resist: how to change management and user resistance to password security. . 2011.
30. Rughini, C. and R. Rughini, Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union. computers security, 2014. 43: p. 111-125.