Refining the Understanding of Usable Security

Wesam Fallatah(✉), Steven Furnell, and Ying He

School of Computer Science, University of Nottingham, Nottingham, UK
{Wesam.Fallatah,Steven.Furnell,Ying.He}@nottingham.ac.uk

Abstract. Cybersecurity technologies and processes must be usable if users are to make effective use of protection. Many security practitioners accept the value of usable security, but few can precisely define it in practice and in terms of how it influences users' security behaviour and the wider security culture in organisations. This paper investigates how different sources characterise usability and usable security to identify the key aspects that affect usability and determine the degree to which usability aspects are relevant in cybersecurity. This has resulted in a definition of usable security and a framework that supports the cybersecurity community's efforts to make security more usable. The motivation for examining the definitions of usable security in detail is to characterise the potential linkage between usable security and the wider security culture within an organization (with the usability of the technology being a factor that could clearly help or impede the acceptance and operation of security, and therefore impact the related culture). The study suggests that, to some degree, the cybersecurity community is catching up with notions that the HCI field has understood for longer. The lack of consistency in defining usable security motivates the proposal of a working definition. Furthermore, a primary outcome of assessing the usability and usable security studies is establishing a framework of usable security, integrating the key aspects identified in the literature. The proposed framework offers a mechanism for operationalising usable security by incorporating principles from both IT/HCI and cybersecurity perspectives.

Keywords: Usability · Usable Security · Security Culture

1 Introduction

There have been significant advancements in developing technical security solutions that would support safeguarding information in organisations. These solutions, however, cannot solely protect organisations and stop cyber threats on their own. Human perceptions and behaviour while interacting with security solutions and other security controls are essential to the overall security systems. According to Verizon [1], the human element is a factor in 82% of data breaches. As a result, organisations started to realise the importance of strengthening security culture as establishing a strong security culture and engaging it can play a crucial role in protecting organisations against breaches. Moreover, security solutions need to be integrated into people's habits, behaviours, and daily actions, i.e., security culture. In order to achieve that, we have to examine the

A. Moallem (Ed.): HCII 2023, LNCS 14045, pp. 49–67, 2023.
https://doi.org/10.1007/978-3-031-35822-7_4

factors that could potentially enable the promotion of good security behaviour and its transition into a security culture. One of the factors to consider is whether making security usable would eventually improve the overall security culture. This study reviews usability definitions from an IT/Human-Computer Interaction (HCI) and cybersecurity perspective by looking into usability definitions and key aspects. In doing so, the study first looks at how usability is defined from both IT/HCI and security perspectives, which led to building a usable security framework that aims to support the efforts of the cybersecurity community to capture the key elements detailed in the HCI studies. The prime outcome of this study conceptualises usable security and offers organisations a practical contribution that they can rely on to strengthen the general security culture.

The remainder of this paper is organised as follows. Section 2 provides an overview of usability and usable security definitions in previous work. A working definition and a framework for usable security are proposed in Sects. 3 and 4, respectively. Section 5 discusses the future work, and Sect. 6 concludes the paper.

2 Defining Usability

The usability of products is essential for functioning, and it affects how users achieve a desired task. In addition, users leave products that are difficult to use and choose alternatives [2]. Thus, creating usable products attracts users and help organisation benefit from users' engagement. To create usable measures, it is vital to understand what characteristics usability entails. This section investigates the various ways in which different sources characterise usability, as a foundation for later discussion of usable security. The goal is to identify what key aspects affect usability and determine the degree to which these aspects are then relevant in cybersecurity.

A comprehensive definition of usability can guide the creation of effective systems and services. Many definitions of usability and its related attributes have been introduced in the literature. It is imperative to note that usability is not a single-dimensional issue, but its attributes connect it to qualities covering many disciplines [3]. Although various usability definitions are discussed in the literature, they nonetheless have attributes in common. Therefore, it is helpful to investigate what characteristics of usability have been identified and what characteristics have the more significant impact on systems' usability in order to consider these while designing usable systems and services. Moreover, Quesenbery [4] believes that it is important to utilise our understanding of each usability dimension to better generate usable products. The International Organisation for Standardisation (ISO) defines usability as the "extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [5]. Still, ISO's definition is not 'universal', and other studies have proposed various usability definitions.

Table 1 demonstrates an illustrative set of usability definitions in an IT/HCI context. The search string: usability AND (definition OR meaning) was formalised to query relevant online indexes and publisher repositories: Springer, Scopus, IEEE Xplore, Web of Science, and Google Scholar. In the search, we considered widely cited data sources that are related to IT/HC and with free access. The list includes sources that suggest a usability definition. However, definitions that are derived from other sources are not taken

into account. Finally, definitions from authoritative sources were also included in the list. For each identified source, the table directly quotes its main definition of usability and then abstracts what are considered to be the key aspects from it. These are then able to be used to show how frequently each aspect was recognised in prior definitions. Most importantly, the resulting data from Table 1 will be crucial in determining how the usability key aspects are relevant in a cybersecurity context and the extent to which these aspects are recognised in usable security studies.

Table 1. Usability definitions and key aspects

Source	Definition	Key aspects
Abran et al. [6]	"a set of multiple concepts, such as execution time, performance, user satisfaction and ease of learning ("learnability"), taken together"	• Execution time/efficiency • Performance • User satisfaction • Ease of learning (learnability)
Bevan and Macleod [7]	"a) the product-centred view of usability: that the usability of a product is the attributes of the product which contribute towards the quality of use; b) the context of use view of usability: that usability depends on the nature of the user, product, task and environment; c) the quality of use view of usability: that usability is the outcome of interaction and can be measured by the effectiveness, efficiency, and satisfaction with which specified users achieve specified goals in particular environments."	• Product • Quality of use • Environment/context • User • Task • Interaction outcome • Effectiveness • Efficiency • User satisfaction • Goals
Bevan et al. [8]	"the ease of use and acceptability of a product for a particular class of users carrying out specific tasks in a specific environment."	• Ease of use • Acceptability • Product • Users • Tasks • Environment/context

(*continued*)

Table 1. (*continued*)

Source	Definition	Key aspects
Constantine and Lockwood [9]	"Usability is influenced by many factors. Highly usable systems are easy for people to learn how to use and easy for people to use productively. They make it easy to remember from one use to another how they are used. Highly usable systems help people to work efficiently while making fewer mistakes. We can think of these characteristics as five facets of usability[…]: - Learnability - Rememberability - Efficiency in use - Reliability in use - User satisfaction"	• Systems • People (users) • Ease of learning (learnability) • Productivity • Fewer mistakes/Error tolerance • Ease of remembering (memorability/rememberability) • Efficiency of use • Reliability of use • User satisfaction
Eason [10]	"the degree to which users are able to use the system with the skills, knowledge, stereotypes and experience they can bring to bear"	• Users • System • Users' skills, knowledge, stereotypes, and experience (user literacy)
EC [11]	"Usability refers to how easy it is to navigate through your website. This is determined by aspects including the way your site arranges and displays information, as well as how comfortable it is for users to interact with it."	• Website • Ease of use • Information display/ user interface • Comfort of use • Interaction
Edwards [12] for Hewlett Packard (hp)	"When using HCI to develop new tech, it was agreed that four main components factor into the equation: the user, the task, the interface, and the context."	• User • Task • User interface • Environment/context

(*continued*)

Table 1. (*continued*)

Source	Definition	Key aspects
Gould and Lewis [13]	"Any system designed for people to use should be easy to learn (and remember), useful, that is, contain functions people really need in their work, and be easy and pleasant to use."	• System • People (users) • Ease of learning (Learnability) • Ease of remembering (memorability) • Useful functions • Use satisfaction
HHS and GSA [14]	"the quality of a user's experience when interacting with products or systems, including websites, software, devices, or applications. Usability is about effectiveness, efficiency and the overall satisfaction of the user"	• User experience (user literacy) • Interaction • Product/system/websites/software/devices/applications • Effectiveness • Efficiency • User satisfaction
Holzinger [15]	"usability is most often defined as the ease of use and acceptability of a system for a particular class of users carrying out specific tasks in a specific environment"	• Ease of use • Acceptability • System • Users • Tasks • Environment/context
IBM [16]	"Usability is the discipline of applying scientific principles to ensure that the application or website being designed is easy to learn, easy to use, easy to remember, error tolerant, and subjectively pleasing"	• Application/website • Ease of learning (learnability) • Ease of remembering (memorability) • Error tolerance • User satisfaction
IEEE [17]	"The ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component."	• Ease of learning (learnability) • User • Input preparation/Output interpretation/ task performance • System/component
IEEE [18]	"the extent to which a product can be used by intended users to achieve specified goals with effectiveness, efficiency, and satisfaction"	• Product • Users • Goal achievement • Effectiveness of use • Efficiency of use • User satisfaction

(*continued*)

Table 1. (*continued*)

Source	Definition	Key aspects
Interaction Design Foundation [19]	"Usability is a measure of how well a specific user in a specific context can use a product/design to achieve a defined goal effectively, efficiently and satisfactorily"	• User • Environment/context • Product/design • Goal achievement • Effectiveness of use • Efficiency of use • User satisfaction
ISO [5] Also adapted by most HCI experts and organisations including [20–24]	"extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"	• System/product/service • Users • Goals achievement • Environment/context • Effectiveness of use • Efficiency of use • User satisfaction
Krug [25]	"making sure that something works well: that a person of average (or even below average) ability and experience can use the thing—whether it's a Web site, a fighter jet, or a revolving door—for its intended purpose without getting hopelessly frustrated"	• Person (users) • Experience (user literacy) • User satisfaction
Microsoft [26]	"Usability is a measure of how easy it is to use a product to perform prescribed tasks."	• Ease of use • Product • Performance • Tasks performance
Nielsen [3]	"usability is not a single, one-dimensional property of a user interface. Usability has multiple components and is traditionally associated with these five usability attributes: - Learnability - Efficacy - Memorability - Errors - Satisfaction."	• User interface • Ease of learning (learnability) • Efficacy • Memorability • Errors tolerance • User satisfaction

(*continued*)

Table 1. (*continued*)

Source	Definition	Key aspects
Preece [27]	"a measure of the ease with which a system can be learned or used, its safety, effectiveness and efficiency, and the attitude of its users towards it"	• Ease of use • Ease of learning (learnability) • System safety • System effectiveness • System efficiency • User attitude/user satisfaction
Quesenbery [4]	"For each of the five dimensions of usability (the 5Es), we think about how it is reflected in requirements for each of the user groups. The 5Es are: - Effective: How completely and accurately the work or experience is completed or goals reached - Efficient: How quickly this work can be completed - Engaging: How well the interface draws the user into the interaction and how pleasant and satisfying it is to use - Error Tolerant: How well the product prevents errors and can help the user recover from mistakes that do occur - Easy to Learn: How well the product supports both the initial orientation and continued learning throughout the complete lifetime of use."	• Effectiveness • Efficiency • Interaction • Users • Goals achievement • User interface • Interaction • User satisfaction • Product • Error tolerance • Ease of learning (learnability)
Schumacher, Lowry [28] for the National Institute of Standards and Technology (NIST)	"the effectiveness, efficiency, and satisfaction with which the intended users can achieve their tasks in the intended context of product use"	• Effectiveness • Efficiency • User satisfaction • Task • Environment/context • Product • User

(*continued*)

Table 1. (*continued*)

Source	Definition	Key aspects
Shackel [29]	"the capability in human functional terms to be used easily and effectively by the specified range of users, given specified training and user support, to fulfil the specified range of tasks, within the specified range of environmental scenarios A convenient shortened form for the definition of usability might be 'the capability to be used by humans easily and effectively', where Easily = to a specified level of subjective assessment Effectively = to a specified level of (human) performance."	• Users • User literacy • Ease of use • Effectiveness of use • User support • Tasks • Performance • Environment/context
Sharp et al. [30]	"usability is generally regarded as ensuring that interactive products are easy to learn, effective to use, and enjoyable from the user's perspective. It involves optimising the interactions people have with interactive products to enable them to carry out their activities at work, school, and in their everyday life. More specifically, usability is broken down into the following goals: - effective to use (effectiveness) - efficient to use (efficiency) - safe to use (safety) - have good utility (utility) - easy to learn (learnability) - easy to remember how to use (memorability)."	• Products • People (users) • Interaction • Activities/tasks • Environment/context • Effectiveness of use • Efficiency of use • Safety • Utility • Ease of learning (learnability) • Ease of remembering (memorability) • User satisfaction

(*continued*)

Table 1. (*continued*)

Source	Definition	Key aspects
Shneiderman and Plaisant [31]	"1. Time to learn: How long does it take for typical members of the community to learn relevant task? 2. Speed of performance: How long does it take to perform relevant benchmarks? 3. Rate of errors by users: How many and what kinds of errors are made during benchmark tasks? 4. Retention over time: Frequency of use and ease of learning help make for better user retention 5. Subjective satisfaction: Allow for user feedback via interviews, free-form comments and satisfaction scales"	• Time of learning/ Ease of learning (learnability) • Speed of performance/ Efficiency • Rate of errors/ Error tolerance • User satisfaction • Task • Users
Usability Professionals Association [32]	"the degree to which something - software, hardware or anything else - is easy to use and a good fit for the people who use it."	• Software/hardware • Ease of use • User satisfaction
Usability.gov [33]	"How effectively, efficiently and satisfactorily a user can interact with a user interface."	• User interface • Effectiveness • Efficiency • User satisfaction • Interaction

Table 1 presents an overview of usability representations from usability studies and authoritative resources. The list has, nonetheless, captured the most significant sources of relevance. The output shown in Fig. 2 supports the conclusion drawn from usability studies, including a systematic review of usability, which covers 790 papers from 2001 to 2018 [34]. The study confirms that the HCI community has primarily adopted ISO's definition of usability and standardised it in an unchanged form. The study also asserts that the most frequently identified usability aspects are "efficiency (70%), satisfaction (66%) and effectiveness (58%)", which are derived directly from the ISO definition. Figure 1 shows the total percentage of the most identified usability key aspects highlighted in our study. Hence, we opt to have consistent vocabularies for the key aspects across all of the sources we are examining, as some of the different terminologies can/may end up being

combined together. For instant, systems, products, websites, software, devices, apps, service, etc. can be characterised as touchpoints. Also, cognitive load, consciousness, and mental image are all defined as 'mental model'. Figure 2 provides a visual insight concerning the most common terms associated with usability generated using an online Word Cloud tool [35] by pasting all the definition text into it to illustrate the most common terms from the definitions presented in the list. A total of 165 occurrences were fed in the key aspects entries. Based upon this grouping, the findings suggest that recognition of the 'touchpoint' is the most considered aspect in usability studies. Also, facets such as 'user satisfaction', 'user', 'efficiency', and 'effectiveness' have been mentioned more repetitively than the other usability aspects.

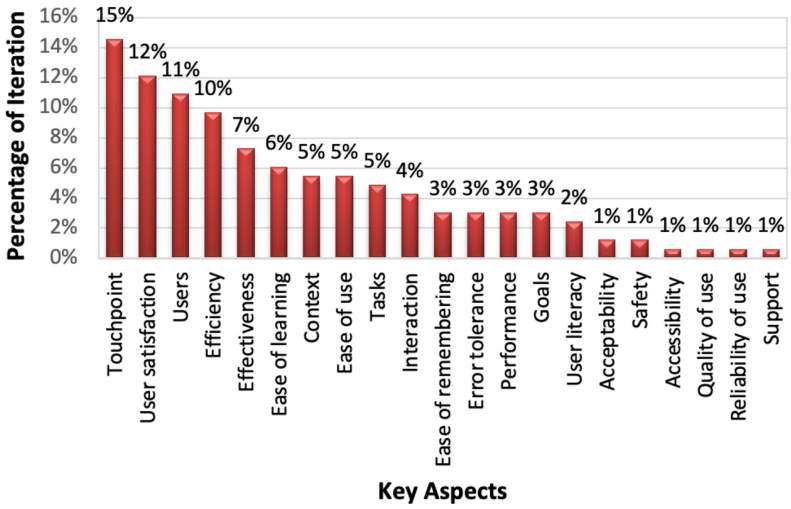

Fig. 1. The total iteration percentage of the terms found related to usability key aspects

Generated using Davies [37]'s Word Cloud Generator.

Fig. 2. Word Cloud denoting prominence of words relating to usability

3 Defining Usable Security

Having determined the key aspects in usability definitions, next we examine how different sources also address usable security to see how the usability aspects are relevant in cybersecurity context. To identify sources that define usable security, the paper took the same approach presented in Sect. 2 above but by using the search string: ("Usable security" OR "Cybersecurity usability" OR "security usability") AND (definition OR meaning). Unlike 'usability' definitions, there do not seem to be many definitions that specifically focus on what it means for a system or service to be both 'usable' and 'secure'. Table 2 presents illustrative examples of existing usable security definitions and the associated key aspects.

Table 2. Illustrative examples of existing usable security definition

Source	Definition	Key aspects
Caputo et al. [36]	"delivering the required levels of security and also user effectiveness, efficiency, and satisfaction"	• Security • User effectiveness • Efficiency • Satisfaction
Zurko and Simon [37]	"security models, mechanisms, systems, and software that have usability as a primary motivation or goal."	• Security models • Mechanisms/system/software • Goal

The definitions in Table 2 are provided as illustrative examples of existing definitions that can be found in usable security related studies. The key aspects associated with these definitions are also highlighted. Table 3 below summarises the key aspects from the definitions suggested by multiple authors, including the two examples in Table 2.

As shown in Table 3, there exists a considerable body of research that aim to represent usable security. There are different perspectives when addressing usable security, and there is no widely accepted formal definition has been observed so far. In addition, few studies clearly outline the different dimensions that may contribute to understanding usable security despite some efforts. Figure 3 shows the total percentage of the most identified usable security key aspects highlighted in our study. Figure 4 provides a visual representation of the most common terms associated with usable security, generated by pasting all of the definition text from the sources shown in Table 3 into an online Word Cloud tool [35].

Compared to usable security, the representation of usability is more consistent in the literature and to some degree, the cybersecurity community is catching up with notions that the HCI field has understood for longer. Figure 3 shows the total percentage of the most identified usable security key aspects highlighted in our study, where a total of 73 occurrences were fed in the key aspects entries. Figure 4 provides a visual insight concerning the most common terms associated with usable security. Notably, 'touchpoints', 'user', 'user satisfaction' are some areas of commonality between usability and usable

Table 3. Summary of usable security key aspects presented in studies

Caputo et al. [37] • Security • User effectiveness • Efficiency • Satisfaction	Theofanos [38] • Cybersecurity • Usability • Interaction	Zurko and Simon [36] • Security models • Mechanisms/system/software • Goal
Johnston, Eloff [39] • User interface / Aesthetic/minimalist design • Visibility • Users • Learnability • Error • User satisfaction • Trust • Environment	Saltzer and Schroeder [40] • User interface • Users • Ease of use • Protection • Mental image • Mechanisms • Goals • Rate of errors/mistakes	Whitten and Tygar [41] • People (users) • Reliability • Tasks • Performance • Errors • User satisfaction • User interface
Hof [42] • Consciousness • Availability/understandability • Empowerment • Activities/Tasks • Interaction • Efficiency • Ease of remembering (memorability) • Interaction • System/application • Support • User satisfaction • Error tolerance • Consistency • Users	Nurse et al. [43] • Accessibility • Users • Support • Error prevention • Visibility • Cognitive load • System/application • Tasks • Performance • User satisfaction • Aesthetic/minimalistic design/user interface • Technical terms • Mental model • Tools	Yee [44] • System/ Software • Explicit Authority (safety related) • Visibility (safety related) • Revocability (safety related) • Path of Least Resistance (safety related) • Expected Ability • Boundaries Appropriation (safety related) • Expressiveness • Clarity • Identifiability, Trusted Path (safety/protection related)

security, whereas important usability aspects such as efficiency and learnability are still considered as outliers in cybersecurity studies. In addition, the 'context of use', which has a degree of importance in usability studies also is not given the required attention from the cybersecurity community. The lack of consistency and clarity in defining and presenting usable security motivates this work to create an initial definition, which will be discussed in the next section.

As a result, this study establishes a working definition of usable security that aims to support the efforts of the cybersecurity community to capture the key elements discussed in the HCI community. The definition is:

'Usable security is utilising usability concepts to enable cybersecurity concepts'

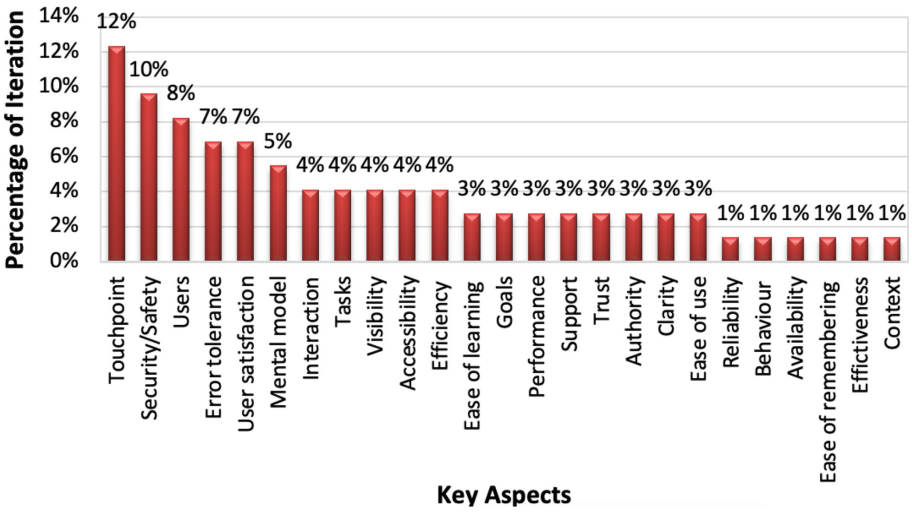

Fig. 3. The total iteration percentage of the terms found related to usable security key aspects

Generated using Davies [37]'s Word Cloud Generator.

Fig. 4. Word Cloud denoting prominence of words relating to usable security

where:

'Usability concepts' = all usability key aspects and requirements,

and

'Cybersecurity concepts' = all cybersecurity aspects and requirements

Furthermore, a primary result arising from our assessment of usability and usable security studies is establishing a framework of usable security, looking at the different

aspects identified in the literature. The perspective of this definition is to be detailed in the usable security framework presented in Sect. 4.

4 Usable Security Framework

A major outcome of reviewing usable security representations is a framework that characterise the relationship between different aspects of usable security (Fig. 5). The framework provides a means to operationalise usable security definiation, taking into account all important facets of usability from both HCI and cybersecurity perspectives.

The main elements of this framework are as follows:

- **User:** a person (expert or non-expert) with expectations/beliefs about the touchpoint they will interact with (i.e., mental model, cognitive model, etc.).
- **Touchpoint:** any point that the user interacts with and creates their experience. This includes digital and physical systems, policies, and procedures.
- **Process:** The action(s) constructed for the user to achieve a goal. The process should be centred on users' needs and meet the usability key aspects based on the context of use.
- **Goal:** a specific aim that users/organisations ought to achieve by considering cybersecurity best practices, each in their context.
- **Context:** the set of conditions that accommodate the process to achieve the goal.

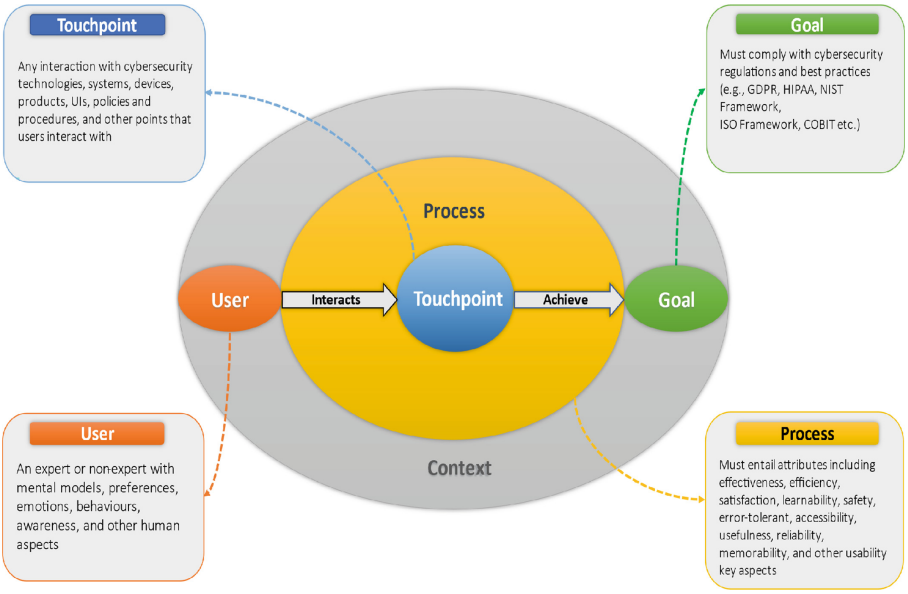

Fig. 5. Usable Security Framework

The framework provides a mechanism to define usable security, taking into consideration all the usability key aspects from both HCI and cybersecurity perspectives. The mechanism implies that a user with a level of experience/awareness/emotions/certain behaviour interacts with a touchpoint (technology, device, product, U.I., etc.) to achieve a goal which should comply with the cybersecurity best practices/requirements in a specified context of use. The process of interaction to achieve the goal should fulfil a set of multiple attributes (i.e. effective, efficient, satisfactory, safe, simple, accessible, reliable, error tolerance, trustworthy, aesthetic, etc.). Organisations can use the existing evaluation methods to assess if the process meets these attributes or if they should value one quality over another based on the context of use and threat modelling process. Also, designers and policy/procedure makers should keep in mind that the touchpoint they create for the user to interact with should make the process cybersecurity compliant.

One example to clarify the operation in the proposed framework is that a user interacts with a banking application using a biometric signature to log into the system to make a bank transfer. In this context, the biometric authentication facilitates a simple, secure, and efficient interaction with the application (touchpoint) to achieve a certain goal in accordance with the best cybersecurity practices. The journey of the user experience once they log in to the system until they make the transfer holds a number of attributes that would leave the user with a positive experience while complying with cybersecurity requirements. Another example is an organisation with a clean desk and clear screen policy, which requires all users to clear their desks at the end of the day and lock their devices' screens as they leave their offices. In this case, the policy is the touchpoint. If a user has to deal with this policy, the organisation is responsible for making the process effective, efficient, and satisfactory. For example, while implementing such a policy, the organisation should provide the employees with clean desk equipment (lockable drawers, storage boxes, etc.) as an alternative to keeping documents lying on the desk.

If it is not usable for users to interact with the touchpoint once they start the process, it will not be guaranteed that the goal they are trying to achieve will comply with best cybersecurity practices because users are always going to find ways to make the touchpoint usable for themselves, which can sometimes damage the whole security system. In many cases, the user cannot be blamed for not abiding by the cybersecurity policies and rules set by organisations if these are not usable while there is a less secure and more usable way to complete a task. Further, some users would be encouraged to bypass the unusable security rules to achieve more important goals (e.g. a doctor bypass/ignore the security system to access a patinate record to save their life.

5 From Usable Security to Security Culture

Examining the concept of usability from both IT/HCI and cybersecurity perspectives contributes into refining our understanding of usable security. It is also a vital step towards characterising the linkage between usable security and security culture. This work further investigates security culture by reviewing the different definitions of security culture presented in studies and the most discussed factors influencing organisations' security culture for the past ten years. There are various definitions of security culture, yet there is no commonly accepted definition. Therefore, most papers suggest a definition

to show how their working definition fits into the overall study. In addition, the research addresses a variety of shared characteristics when investigating factors that impact establishing and maintaining strong security culture. Many studies emphasise the importance of top management and leadership support. This support is arguably critical in enforcing and fostering other factors such as increasing awareness and knowledge, applying policies and procedures, and complying with corporate governance [45–47]. Cybersecurity activities may not seem important without the support from top management; therefore, management must guide employees' security culture efforts and manage resources effectively [48]. Despite the importance of top management's support for cybersecurity awareness and training programs, a recent study suggests that compliance is the primary driving factor while conducting awareness and training programs because regulations require businesses to provide regular cybersecurity awareness and training programs [49].

Policies and procedures also appear in many papers as a vital factor. It is worth noting that policies and procedures are frequently associated with users' awareness and knowledge, and the training programs organisations offer to their employees. For example, Chen, Ramamurthy [50] assert that security education, training, and awareness programs are key components that influence employees' understanding of organisational security policy and that the awareness will ultimately positively impact the overall security culture. By contrast, the lack of awareness and knowledge to implement the necessary policies and procedures might negatively impact the organisation's security culture. Other factors, such as change management, communication, trust, technological aspects, and national culture, also appear in multiple studies. However, a further important implication is to consider all internal (e.g., management and awareness) and external (e.g., national culture and technological) factors while establishing and maintaining robust security culture, besides determining the degree to which the organisation's security culture is dependent on each of them [47].

Notably, no study has directly stated the usability of security as a factor influencing security culture, although few studies identify usability as an embedded/integrated quality in other factors. For example, Furnell and Rajendran [51] emphasise that usability is an aspect that can enhance user behaviour, Padayachee [52] asserts that usability increases the likelihood of compliance, and Hassan and Ismail [53] discuss how change management improves security through multiple elements including usability. Although previous studies consider some aspects of usable security, no explicit connection is identified between usable security and security culture. Further, a practical implication is to assess the security culture in organisations and determine the extent to which a particular factor impacts cultivating a strong security culture. We plan to continue this work by designing a means to assess the influence of usable security on security culture. This can be achieved by creating a security culture framework focusing on the usability aspect as an enabler. Also, to further examine security culture representation in studies in terms of definitions, influential factors (e.g., significant factors, contributing factors, and marginal factors), and measurement approaches then to identify whether taking a usable security approach can help them maintain good security culture.

6 Conclusions

Significant progress has been made in creating technical security solutions that would help organisations mitigate serious security risks. However, on their own, these solutions are unable to fully safeguard organisations against threats. The effectiveness of the overall security systems depends on how people perceive and behave while dealing with security solutions and other security measures. As a result, security studies and security professionals began to realise the need to investigate factors that can strength security culture in organisation. One way to establish and maintain a strong security culture is to consider a usable security approach. As a method of achieving this, we proposed a definition of usable security. Without a clear definition of usable security, it becomes difficult to identify how to implement security measures that are both secure and usable. A usable security framework then accompanied the definition to provide a structured approach that supports previous studies' efforts and helps ensure that all relevant usability aspects are considered while implementing security measures. Further, Organisations can take cybersecurity safeguards without falling into usability mistakes that often accompany their implementation. Consequently, users will be able to make informed decisions about the measures they are asked to follow and comply with, which can presumably be a major factor in fostering a robust security culture. Additionally, there does not seem to be a specific single definition of security culture that is widely acknowledged. However, most publications include definitions to demonstrate how their working definitions fit into the larger research. Moreover, the characteristics of security culture appeared to be a topic of considerable interest in the literature. Although many studies highlighted the significance of usable security, previous research did not specifically investigate the linkage between usable security and security culture.

References

1. Verizon: 2022 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/. Accessed 10 July 2022
2. Nielsen, J.: Usability 101: Introduction to Usability (2012). https://www.nngroup.com/articles/usability-101-introduction-to-usability/
3. Nielsen, J.: Usability Engineering. Morgan Kaufmann (1993)
4. Quesenbery, W.: Using the 5Es to Understand Users - Whitney Interactive Design. WQusability - Whitney Quesenbery (n.d.). https://www.wqusability.com/articles/getting-started.html. Accessed 15 Feb 2022
5. ISO. Ergonomics of human-system interaction—Part 11: Usability: Definitions and concepts (2018). https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en
6. Abran, A., Khelifi, A., Suryn, W., Seffah, A.: Usability meanings and interpretations in ISO standards. Softw. Qual. J. **11**(4), 325–338 (2003)
7. Bevan, N., Macleod, M.: Usability measurement in context. Behav. Inf. Technol. **13**(1–2), 132–145 (1994)
8. Bevan, N., Kirakowskib, J., Maissela, J.: What is usability. In: Proceedings of the 4th International Conference on HCI. Citeseer (1991)
9. Constantine, L.L., Lockwood, L.A.: Software for Use: A Practical Guide to the Models and Methods of Usage-Centered Design. Pearson Education (1999)
10. Eason, K.D.: Information Technology and Organizational Change. CRC Press (1989)

11. European Commission. Usability. Internal Market, Industry, Entrepreneurship and SMEs. https://ec.europa.eu/growth/sectors/tourism/business-portal/usability_en. Accessed 17 Feb 2022
12. Edwards, M.: Exploring Human-Computer Interaction. HP (2018). https://www.hp.com/us-en/shop/tech-takes/exploring-human-computer-interaction. Accessed 15 Feb 2022
13. Gould, J.D., Lewis, C.: Designing for usability: key principles and what designers think. Commun. ACM **28**(3), 300–311 (1985)
14. HHS and GSA: The Research-Based Web Design & Usability Guidelines, Enlarged/Expanded edition. U.S. Government Printing Office. https://www.usability.gov/what-and-why/usability-evaluation.html. Accessed 31 Jan 2022
15. Holzinger, A.: Usability engineering methods for software developers. Commun. ACM **48**(1), 71–74 (2005)
16. IBM. User Experience. Usability (2008). https://www-03.ibm.com/services/ca/en/mobility/offerings_userexperience_usability.html#:~:text=Usability%20is%20the%20discipline%20of,error%20tolerant%2C%20and%20subjectively%20pleasing. Accessed 15 Feb 2022
17. IEEE. IEEE Standard Glossary of Software Engineering Terminology (1990). https://ieeexplore.ieee.org/document/159342/definitions#definitions. Accessed 27 Feb 2022
18. IEEE. Usability and Accessibility (2022). https://brand-experience.ieee.org/guidelines/digital/style-guide/usability-and-accessibility/. Accessed 27 Feb 2022
19. Interaction Design Foundation. Usability (2022). https://www.interaction-design.org/literature/topics/usability#:~:text=Usability%20is%20a%20measure%20of,deliverable%E2%80%94to%20ensure%20maximum%20usability. Accessed 27 Feb 2022
20. HFES. Human Readiness Level Scale in the System Development Process (2021)
21. ANSI. Ergonomics of Human-System Interaction - Part 11: Usability: Definitions and Concepts (2022). https://webstore.ansi.org/standards/iso/iso9241112018?_ga=2.3299568.111955288.1644355252-1926938011.1644355252. Accessed 20 Feb 2022
22. BSI, Ergonomics of human-system interaction - Usability: Definitions and concepts. https://shop.bsigroup.com/products/ergonomics-of-human-system-interaction-usability-definitions-and-concepts/tracked-changes. Accessed 20 Feb 2022
23. Jordan, P.W., Thomas, B., McClelland, I.L., Weerdmeester, B.: Usability Evaluation in Industry. CRC Press (1996)
24. IEC. Usability (2018). https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=871-01-08. Accessed 15 Feb 2022
25. Krug, S.: Don't Make Me Think!: A Common Sense Approach to Web Usability. Pearson Education India (2000)
26. Microsoft, Usability in Software Design (2019). https://docs.microsoft.com/en-us/windows/win32/appuistart/usability-in-software-design#defining-usability. Accessed 11 Feb 2022
27. Preece, J.: A Guide to Usability: Human Factors in Computing. Addison-Wesley Longman Publishing Co., Inc. (1993)
28. Schumacher, R.M., Lowry, S.Z., Schumacher, R.M.: NIST guide to the processes approach for improving the usability of electronic health records. US Department of Commerce, National Institute of Standards and Technology (2010)
29. Shackel, B.: Usability-context, framework, definition, design and evaluation. Interact. Comput. **21**, 339–346 (2009)
30. Sharp, H., Rogers, Y., Preece, J.: Interaction design: beyond human-computer interaction (2019)
31. Shneiderman, B., Plaisant, C.: Designing the User Interface: Strategies for Effective Human-Computer Interaction. Pearson Education India (2010)
32. Usability Professionals Association (2010). What is Usability? https://www.usabilitybok.org/what-is-usability. Accessed 15 Feb 2022

33. Usability.gov. Glossary: Usability. https://www.usability.gov/what-and-why/glossary/u/index.html. Accessed 15 Feb 2022
34. Weichbroth, P.: Usability of mobile applications: a systematic literature study. IEEE Access **8**, 55563–55577 (2020)
35. Davies, J.: Word Cloud Generator. https://www.jasondavies.com/wordcloud/. Accessed 25 May 2022
36. Caputo, D., Pfleeger, S., Sasse, M., Ammann, P., Offutt, J., Deng, L.: Barriers to usable security? Three organizational case studies. IEEE Secur. Priv. **14**, 22–32 (2016)
37. Zurko, M., Simon, R.: User-centered security. In: Proceedings of the 1996 Workshop on New Security Paradigms (1996)
38. Theofanos, M.: Is usable security an oxymoron? IEEE Comput. **53**(2), 71–74 (2020)
39. Johnston, J., Eloff, J.H., Labuschagne, L.: Security and human computer interfaces. Comput. Secur. **22**(8), 675–684 (2003)
40. Saltzer, J., Schroeder, M.: A proteção de informação em sistemas de computador. Proc. IEEE **63**(9), 1278–1308 (1975)
41. Whitten, A., Tygar, J.: Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: USENIX Security Symposium (1999)
42. Hof, H.-J.: User-centric IT security-how to design usable security mechanisms. arXiv preprint arXiv:1506.07167 (2015)
43. Nurse, J., Creese, S., Goldsmith, M., Lamberts, K.: Guidelines for usable cybersecurity: past and present. In: Third International Workshop on Cyberspace Safety and Security (CSS) (2011)
44. Yee, K.-P.: User interaction design for secure systems. In: Deng, R., Bao, F., Zhou, J., Qing, S. (eds.) ICICS 2002. LNCS, vol. 2513, pp. 278–290. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-36159-6_24
45. Mahfuth, A., Yussof, S., Baker, A., Ali, N.: A systematic literature review: Information security culture. In: 2017 International Conference on Research and Innovation in Information Systems (ICRIIS). IEEE (2017)
46. AlHogail, A., Mirza, A.: Information security culture: a definition and a literature review. In: 2014 World Congress on Computer Applications and Information Systems (WCCAIS). IEEE (2014)
47. Da Veiga, A., Astakhova, L., Botha, A., Herselman, M.: Defining organisational information security culture—perspectives from academia and industry. Comput. Secur. (2020)
48. Uchendu, B., Nurse, J., Bada, M., Furnell, S.: Developing a cyber security culture: current practices and future needs. Comput. Secur. **109**, 102387 (2021)
49. Bada, M.: Stakeholder Analysis: Motives, Needs, and Drivers for Cybersecurity Awareness Training in Modern Work Environments, in AwareGO (2022)
50. Chen, Y., Ramamurthy, K., Wen, K.-W.: Impacts of comprehensive information security programs on information security culture. J. Comput. Inf. Syst. **55**(3), 11–19 (2015)
51. Furnell, S., Rajendran, A.: Understanding the influences on information security behaviour. Comput. Fraud Secur. 12–15 (2012)
52. Padayachee, K.: Taxonomy of compliant information security behavior. Comput. Secur. 673–680 (2012)
53. Hassan, N., Ismail, Z.: A conceptual model for investigating factors influencing information security culture in healthcare environment. Procedia-Soc. Behav. Sci. 1007–1012 (2012)