JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2023, 1–15
https://doi.org/10.1093/cybsec/tyad010
Research paper

Research paper

The security mindset: characteristics, development, and consequences

Koen Schoenmakers[1,†], Daniel Greene[2,*,†], Sarah Stutterheim[3], Herbert Lin[4] and Megan J. Palmer[5]

[1]Department of Psychology, Harvard University, Cambridge, MA 02138, USA, [2]Gryphon Scientific LLC, 6930 Carroll Ave., Takoma Park MD 20912, and Center for International Security and Cooperation, Stanford University, Stanford, CA 94305, USA, [3]Care and Public Health Research Institute & Department of Health Promotion, Faculty of Health, Medicine, and Life Sciences, Maastricht University, 6200 MD, Maastricht, the Netherlands, [4]Center for International Security and Cooperation, Stanford University, Stanford, CA 94305, USA and [5]Department of Bioengineering and Center for International Security and Cooperation, Stanford University, Stanford, CA 94305, USA

*Correspondence address. 6930 Carroll Avenue, Suite 810 Takoma Park, MD 20912. Tel: +570-856-1216; E-mail: dgreene@gryphonscientific.com

†The authors wish it to be known that, in their opinion, the first two authors should be regarded as co-first authors.

Received 4 May 2022; revised 16 December 2022; accepted 3 April 2023

Abstract

The world is facing a cybersecurity skills gap as cybercrime and cyberwarfare grow in importance. One often-discussed quality that is potentially relevant to cybersecurity recruitment and education is the so-called "security mindset": a way of thinking characteristic of some security professionals that they believe to be especially advantageous in their work. Although some employers express a desire to hire people with a security mindset, and initiatives to cultivate the security mindset are being implemented, it has no common definition and little is known about its characteristics, its development, and its consequences. We interviewed 21 cybersecurity professionals who strongly identified as having a security mindset based on a minimal description drawn from existing literature. Thematic analysis of the interview data suggests that the security mindset can be conceptualized as consisting of three interconnected aspects—"monitoring" for potential security anomalies, "investigating" anomalies more deeply to identify security flaws, and "evaluating" the relevance of those flaws in a larger context. These three aspects develop in different ways and have different personal and professional consequences. Participants mostly spoke positively of the security mindset, but they also mentioned several disadvantages not mentioned by existing security-mindset literature, such as mental health pressures, workplace tensions, and negative effects on personal relationships. We discuss the implications of these findings for future study of the security mindset and suggest practical implications for cybersecurity management, education, and recruitment.

Key words: security mindset, cybersecurity, management, awareness, psychology, cyberpsychology, motivation, culture

Introduction

Background

> "Security requires a particular mindset. Security professionals—at least the good ones—see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it."
>
> – Bruce Schneier, 2008 [1].

The globe is facing a shortage of competent cybersecurity professionals, referred to as the cybersecurity "skills gap" [2–4]. According to a recent estimate, there are ∼2.72 million cybersecu-

rity jobs in demand worldwide [5]. Meeting the demand for cybersecurity requires breaking down cybersecurity expertise into component skills and qualities that can be clearly identified and cultivated [6–10].

One often-mentioned quality of some cybersecurity professionals is called the "security mindset"—a certain way of thinking that is seen as advantageous in cybersecurity work and that tends to involve constantly searching for security flaws in nearby systems. Being a security professional is claimed to be neither necessary nor sufficient to have a security mindset [1, 11], but industry insiders indicate that they look for a security mindset when recruiting and try to cultivate it among their employees [12–14]. Several cybersecurity education programs also devote attention to it, and it is included in US cybersecurity curricula [6, 15, 16].

However, despite this interest, the security mindset has not yet been clearly conceptualized [11, 17, 18]. There have been some written case studies of attempts to teach the security mindset, but they have avoided the challenge of precisely conceptualizing and measuring its presence, relying instead on indirect measurements such as code quality or teaching evaluations [17, 19–21]. Without conceptual clarity, the security mindset cannot be effectively measured, taught, or linked to existing social science research.

Many other questions about the security mindset also remain empirically underexplored. How does the security mindset develop? Can it be deliberately cultivated, or is it relatively fixed or innate? Does it indeed contribute to improved cybersecurity performance, is it merely correlated with other qualities that drive performance, or is it uncorrelated with performance entirely? Are there any negative personal or social consequences of having a security mindset? In an influential 2008 article in *Wired* magazine and subsequent blog comments, cybersecurity professional Bruce Schneier posed some of these questions, but little work has been done since then to investigate further [1].

We view the security mindset as a psychological phenomenon that deserves more careful scrutiny, and we believe that the field of social psychology is well-positioned to provide it. Social psychologists have a successful track record of studying psychological phenomena that are well-known within specialized professional communities. Some examples include mindfulness among meditators, "choking under pressure" among athletes and other top performers, and the sense of belonging in academic settings among students and educators [22–24]. In each case, psychologists have conducted qualitative research to understand phenomena from the perspectives of the people experiencing them, translated their understanding into quantitative measures, demonstrated links between those measures and valued outcomes, and developed scalable programs for training and improvement [25–27].

We hope that formal study of the security mindset can both offer theoretical contributions and help to meet global demand for cybersecurity expertise. Following general best-practices in applied social psychology research [28, 29], we begin by conducting what, to our knowledge, is the first qualitative study of cybersecurity professionals' own perspectives on their self-identified security mindsets. We aim to answer the following questions:

1. How do cybersecurity professionals who self-identify as having a "security mindset" conceptualize its meaning, including its components and characteristics?
2. How do they believe that the security mindset is developed?
3. What do they believe are the personal and professional consequences of having a security mindset?

Related work

There is no common definition of the security mindset and there is little agreement about its nature as a psychological construct. For example, the security mindset has been described as a unitary ability or set of abilities [17, 19, 30, 31], as a character trait or set of traits [1, 32], and as a set of attitudes, beliefs, and/or values [11, 18]. However, some consistent themes emerge across the literature. We review two central themes below in order to frame our own approach to the topic.

Common features of the security mindset

First, whether it is defined as an ability, trait, belief, value, or habit, most existing discussions of the security mindset emphasize that it involves engaging in an active cognitive process to identify security vulnerabilities. One phrase that is frequently used when describing the security mindset is "thinking like an attacker" [1, 19, 31–33]. It has also been described as "think[ing] about failures and how to trigger them" [17] and "recognizing how something can be used maliciously or broken" [34]. Similarly, a set of cybersecurity curricular guidelines created by the Joint Task Force on Cybersecurity Education define "adversarial thinking," also described as an "adversarial mindset," as "a thinking process that considers the potential actions of the opposing force working against the desired result" [6].

Second, most discussion of the security mindset emphasizes that it is proactive and intrinsically motivated, above and beyond the demands of work. For example, Schneier's original description of the security mindset (and the enthusiastic comment threads that followed) emphasized the idea that some people "just can't help" constantly looking for security flaws in both work and daily life [1, 32]. The security mindset has also been described in emotional terms as "a peculiar mix of curiosity and paranoia that turns life into a perpetual game of asking 'what if' questions" [13]. The emphasis on the motivational aspect of the security mindset is consistent with extensive prior work on the importance of motivation to engage in cybersecurity practices [35–39].

Related concepts

Culture plays a pervasive role in shaping behavior, and security-related behavior is no exception [40, 41]. Organizational culture motivates individuals to engage in cybersecurity practices [42–45]. For example, organizations that emphasize personal responsibility for writing secure code or that appoint "security champions" appear to influence the coding practices of their employees [45–47]. It is therefore important to understand if and how cultural factors both in and out of work lead people to adopt a security mindset.

In one of the few empirical studies of the security mindset, Haney et al. examined cultural influences on the security mindset by interviewing individuals working at a company that develops cryptographic products [33]. They found that participants cultivated a personal commitment to cybersecurity that was heavily influenced by their surrounding "security culture," which they defined as "a subculture of an organization in which security becomes a natural aspect in the daily activities of every employee." However, Haney et al. also freely used the term "security mindset" to describe characteristics of both individuals and entire organizations, making it difficult to conceptually separate "security mindset" from "security culture" in their framing. For clarity and consistency with most other work, we use the term "security mindset" to refer to a property of individuals and not groups. We discuss the role of cultural factors further in "Development of the security mindset" and in the discussion.

The security mindset is also related to, but distinct from, several individual-level constructs studied by cybersecurity scholars and so-

cial psychologists. One is specialized technical knowledge about systems or general experience in the security field. Several authors and curricular guidelines have proposed that technical knowledge is helpful or perhaps even necessary for a security mindset, but not sufficient [1, 6, 17, 19, 31]. Our model of the security mindset is consistent with these claims; as we describe below, the different aspects of the security mindset are not synonymous with technical knowledge. The security mindset is also distinct from security self-efficacy, or the perception of one's own level of security ability [48]. While it may contribute to security self-efficacy, the security mindset itself is commonly described as an active process rather than a judgment of one's own ability.

Finally, the security mindset partially resembles psychological models of threat perception and response that have been used to predict cybersecurity-related behavior, such as protection motivation theory (PMT) and the extended parallel process model (EPPM) [35, 49, 50]. These models are intended to explain the possible responses that people have to threats and fear appeals, such as taking protective action or engaging in coping strategies, based on factors such as the perceived severity of the threat and one's ability to respond. Unlike PMT and EPPM, the security mindset appears at first glance to be a process of proactively seeking out possible security threats rather than a process of responding to them. However, as we describe below, many of our study participants described an aspect of the security mindset dedicated to evaluating the severity of threats once they are discovered. Thus, careful accounts of the security mindset may inform and integrate smoothly with models of threat perception by describing both how threats are identified and how they are appraised.

Limitations and present work

In summary, most existing literature on the security mindset describes individuals who look for security flaws in systems around them in a proactive, self-motivated fashion. But beyond this, many basic questions remain about the exact nature of the security mindset. For example, little is known about the specific ways of thinking that enable some people to spot security flaws. With the exception of Haney et al. [33], there is also little discussion of the origins of the security mindset and why it seems to be so motivating to some people and not others. There are no survey measures of the security mindset that could be used to identify and cultivate it, and scholars disagree about whether it can be taught at all [1, 20, 21]. Finally, there is little discussion of the consequences of a security mindset for one's personal and professional life. For example, the security mindset is claimed to be helpful in cybersecurity roles, but heightened sensitivity to risks and potential attackers could also be a source of personal stress and worry [51, 52].

An underlying problem with most of the literature on the security mindset is the lack of empirical data [1, 11, 13, 17–19, 31, 32]. The few articles with empirical data only touch briefly on the topic of the security mindset [33, 34] or describe teaching interventions without including the security mindset itself as an outcome measure [20, 21].

When the existing literature does not adequately address a phenomenon, interviews with a target population may be used to gain more clarity [53]. To develop a more empirically grounded understanding of the security mindset while building on previous work, we distilled the common themes described above into a minimal description of the security mindset that matches most current sources on the topic: "the tendency to look for and think about security flaws in the systems around oneself, even when one is not directly instructed to do so." Because we lacked an existing measure for (or even a precise definition of) this tendency, we instead sought out cybersecurity professionals who self-identified as having a security mindset by this description and then allowed them to elaborate further on the topic in semi-structured interviews. We believe that it was helpful to provide participants with our minimal description because they might have otherwise confused the term "security mindset" with something like a general "knack" for security or security self-efficacy [48].

Methods

Sampling and recruitment

We recruited cybersecurity professionals via purposive and snowball sampling using an email advertisement sent to a cybersecurity reading group email list (Appendix A). (The list is based at Stanford University but includes external affiliate members who are invited at the discretion of current members. It contained ∼120 members as of May 2022.) The outreach email asked for cybersecurity professionals who self-identified as having a security mindset according to the minimal description provided above. We also included a list of examples of possible security mindset behaviors from informal conversations with cybersecurity professionals and advisors to make the description more concrete.

The outreach email led to an intake survey with more information and qualification questions (Appendix B). In our intake survey, as a double-check, we asked potential participants about the extent to which they identified with the security mindset as described, and we only retained participants who answered in the top two scale points on a five-point scale ("quite a lot" or "a great deal"). One potential participant was excluded through this process. Participants chose from a list of job roles from the Canadian Centre for Cyber Security (CCCS) Workforce Development and Curriculum Guide, which consists of 35 specific roles grouped into four domains [54]. In order to participate, participants had to be currently employed as a cybersecurity professional.

During the recruitment phase, we monitored the spread of different roles included in our sample to make sure that a variety of different roles and domains were included. We also asked participants who had completed interviews to suggest other cybersecurity professionals they knew who might be interested in participating, and we contacted them with the same email advertisement.

We ultimately recruited 21 participants, all from the USA. The majority of the sample identified as male ($n = 17$) and White ($n = 18$); 4 participants identified as female and 3 identified as Asian or Pacific Islander ($n = 3$), the only non-White racial/ethnic category represented in the sample. Participants played a variety of roles within the cybersecurity industry, spanning all four domains listed in the CCCS's Workforce Development and Curriculum Guide (Table 1). Many participants indicated that roles within cybersecurity are not rigidly demarcated, that they identified with multiple roles in CCCS's guide, and that throughout their career they had fulfilled multiple roles spanning different domains. The largest group of participants had spent a large part of their career in IT, but the sample included a number of divergent occupational backgrounds, including the military, law enforcement, politics, academia, and manual labor.

Procedure

This study was approved by the Stanford University Institutional Review Board before recruitment (Protocol #60 764). After initial recruitment and the intake survey, 21 semi-structured interviews were conducted by one or both of the two main researchers over Zoom. Before starting interviews, participants were asked to review and sign an informed consent form. Interviews lasted ∼1–2 hours [mean: 1:40; min: 0:46; max: 2:42]. Audio was recorded over Zoom.

Table 1: Three: aspects of self-identified security mindset mentioned by participants ($n = 21$), ordered based on their professional roles as demarcated by the CCCS.

Job category	Job title	Monitoring	Investigating	Evaluating
Design & develop	Cyber security researcher			
	Cyber security researcher	x	x	x
	Security architect	x	x	x
	Security engineer	x	x	x
	Security engineer	x	x	x
Govern & support	Chief information security officer	x	x	
	Chief information security officer	x	x	x
	Chief information security officer		x	x
	Chief information security officer	x	x	x
	Chief information security officer	x	x	x
	Cyber security manager	x	x	x
	Cyber security manager	x	x	x
	Cyber security manager	x	x	x
	Project manager	x	x	x
Protect & defend	Incident responder/handler	x	x	x
	Incident responder/handler	x	x	
	Penetration tester		x	
	Cyber security analyst	x	x	
	Cyber security analyst	x		
Operate & maintain	Network security operator/specialist	x	x	
	Technical support specialist		x	

The participant in the first row of the table is an outlier; they mentioned all three of the aspects noted above, but did not conceptualize them as being part of their security mindset (see section 3.2).

The interviews were guided by an interview protocol consisting of open-ended questions and follow-up probes (Appendix C). This protocol was derived from three pilot interviews with cybersecurity professionals, which are not included in the data. The final interview protocol included questions on three broad topics corresponding to our research questions: personal definitions and characteristics of the security mindset, the development of participants' security mindset, and the personal and professional consequences of the security mindset for participants. Throughout the interviews, the focus was on participants' own security mindsets, but the conversations also included discussion of the security mindsets of other people, such as employees, colleagues, family, and the public. After completing each interview, participants were given the option to be paid $30/hour for participation in the study in the form of digital gift cards sent to their email addresses, scaled to the duration of the interview. All interviews were conducted between June and August 2021.

Data processing and analyses

We transcribed the audio recordings of the interviews using the transcription software Otter.ai. Both main researchers listened to all of the interview recordings at least once, reviewing the transcripts for mistakes. We then analyzed the data with the qualitative analysis software MaxQDA + 10 using an inductive and reflexive approach, following the thematic analysis approach of Braun and Clarke [55]. Thematic analysis consists of six phases: familiarization with the data, coding, theme generating, theme review, theme naming, and write up [56]. Lines of text of the interview were labeled with codes. These codes had a semantic focus, rather than a latent one, meaning that codes represented the explicit "surface level" meaning of a line of text rather than any implicit underlying meaning [55]. Both main researchers engaged in this analysis, checking each other's work and meeting regularly to discuss. Semantic codes were grouped into themes, and these themes were discussed among the main researchers and with the wider research team for a critical evaluation. Lastly, the resulting themes were given finalized names. These phases are iterative rather than chronological, meaning that we moved back and forth between them before reaching our final results. The primary goal of our research was to discover recurring and emerging themes rather than establishing a precise level of agreement, which would be appropriate for a more confirmatory approach to analysis. Therefore, following established practices in qualitative research [57], we decided that calculating inter-rater agreement was not appropriate for this study.

During analysis, we found that participants' responses about their conceptualization of the security mindset could be grouped into three themes, which we labeled "monitoring," "investigating," and "evaluating." We also coded themes related to participants' self-reported development of their security mindsets, their motivations for engaging the mindset, and the personal and professional consequences of engaging the mindset. We compared these latter themes with the three conceptual themes across participants in order to identify variations in the development, motivation, and consequences of the security mindset across the categories of monitoring, investigating, and evaluating. For example, we were able to identify curiosity as a common self-reported motivation for investigating, but not for evaluating.

Finally, we use pseudonyms when attributing quotes below in order to protect the anonymity of the participants. Quotes that contain potentially sensitive information were left entirely unattributed to prevent readers from inferring their origins by comparing multiple quotes from the same pseudonym.

Results

Three aspects of the security mindset

Participants tended to define the security mindset in terms of three distinct but interrelated aspects. These are (i) an unconscious habit of

monitoring for potential security flaws, (ii) a conscious *investigating* of systems to confirm security flaws, and (iii) *evaluating* the seriousness of a given flaw in a larger context.

All but one participant described at least one of the three aspects, but different participants included different aspects into their own definitions, and we found all possible combinations of the three aspects in our sample. Most participants associated all three aspects with the term "security mindset" but emphasized their own proclivity for one of them.

Monitoring

When describing their security mindsets, most participants said that they automatically, unconsciously, and uncontrollably spotted potential security flaws in the digital, physical, and social worlds around them. We call this process "monitoring." Many participants said that they are always monitoring, even when not in a work context. They described monitoring in terms of a heightened sensitivity for cues that could reveal security vulnerabilities upon further inspection.

> And that security mindset, I think about it as sort of like a spidey sense, right? It's not something that you're thinking about in your forebrain, but it's always kind of percolating in the back. Once you start to see things in the world through that lens, then everything kind of… you can't help yourself, everywhere you go, you know, you're in the airport, you see a machine and you think of [potential vulnerabilities]. (Jonathan)

Participants drew from their areas of expertise in their monitoring. For example, participants with an information and communications technology background tended to monitor more for cues that could suggest digital vulnerabilities, such as suspicious URLs or email requests, while those with a military or law enforcement background were more likely to mention cues that could suggest physical vulnerabilities like unlocked doors or suspicious strangers. For example, one participant with a military background said "Do you remember the shooting that happened in Las Vegas? […] So now that's part of my threat landscape now. Now I'm also looking for high windows." However, most participants reported being attentive to potential security vulnerabilities in both domains.

Many participants also monitored for cues that were unexpected but not immediately suggestive of potential security flaws. One participant mentioned, "Any time you notice something that is outside of the expected behavior, that's a trigger." In the digital domain, this could be a web page that loads in an unexpected manner or an unusual error message. In the physical domain, one participant described a situation in which he did not find anyone in a street that he expected to be busy. While some people might not think twice about such an observation, for this participant it acted as a trigger to engage in "investigating," which we describe below.

Investigating

Participants also described a second, distinct, and more conscious mental process that becomes active once they have noticed something unusual while monitoring. We call this second process "investigating." Investigating involves "thinking like an attacker"—expending mental effort to learn if a certain cue is in fact a sign of an actual security vulnerability.

> It's not like I look at a system and can immediately list out the 800 ways I can break it, I just have to sort of be like… "Oh, wonder if this would work?" or "Wonder if that's like…?" […] And that's where I think I would take the next step. (Bob)

Many participants used spatial metaphors such as "pathways" and "routes" to describe the different mental steps they would think through, as if they were mentally simulating navigating an imaginary space. According to participants, the process of investigation may be entirely mental, but it could also involve probing real systems, such as trying to enter a password-protected page by inputting code or trying to open supposedly locked doors.

Investigating was particularly emphasized by "Protect & Defend" roles such as penetration testers, but it was also the most commonly mentioned aspect of the security mindset overall. Some participants described that the process of investigating has become so automatic that it sometimes happens almost instantaneously. With experience, a participant might go in a split second from monitoring, to investigating, to identifying a security flaw. In fact, some participants blurred the distinction between monitoring and investigating, with one participant saying "I would have a tendency to see the failure modes of something even before engaging with it."

Evaluating

Many participants made the point that perfect security is impossible. Most large systems will have an uncountable number of potential weaknesses for attackers, and some will never be found. Time and cognitive resources are scarce, and therefore one cannot engage with every single cue one encounters. It is better to prioritize which investigations are worth one's efforts. We call this process "evaluating," and several participants described it as an important element of their security mindset. For example, one participant said "A security mindset, it gives you an opportunity to help sorting or stack-ranking the things that you would start with." Participants described evaluating in terms of intuiting the likelihood and magnitude of harm associated with a given security threat in order to arrive at a judgment on how to proceed:

> So there's the first aspect of, like, "recognize what all the possibilities are," and that's really the immature security mindset, right? Which is like, where you realize, "Oh, crap, I've got [metaphorical] doors and windows all over!" […] But then the next level is like looking at it from a very pragmatic standpoint: What is the likelihood of that, right? Because you're looking at threat, vulnerability, likelihood, you're looking at all those things all combined together, to determine risk. (Vincent)

Some participants described evaluating as a more conscious process, while others described it as more of an unconscious and intuitive judgment. Several participants also mentioned that it was helpful for them to consider what one called the "drives, motivations, incentives, and goals" of potential attackers in order to properly evaluate security flaws.

Of the three aspects, evaluating was the least-frequently mentioned. It was emphasized most by participants in "Govern & Support" and "Design & Develop" roles, such as Chief Information Security Officers (CISOs) and cybersecurity managers, and less so by participants in more front-line "Protect & Defend" and "Operate & Maintain" roles.

An integrated view

Despite the differences in emphasis between the three aspects of the security mindset, participants described them as mutually reinforcing in a number of ways, summarized in Figure 1 below. When integrating these aspects, a coherent picture arises of the security mindset as made up of three distinct but interlocking processes.

Participants described monitoring and investigating as working hand-in-hand. Unconscious and habitual monitoring for security

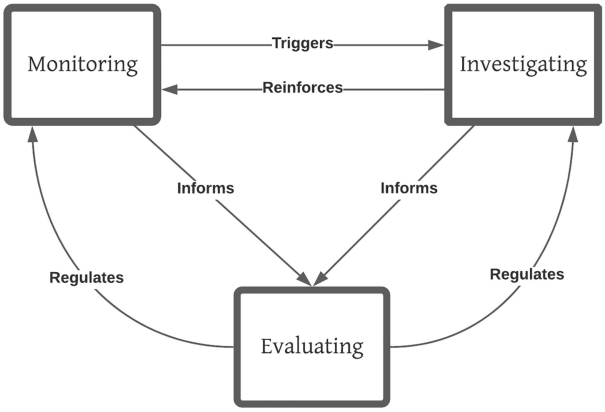

Figure 1: Relationships between aspects of the security mindset described by participants. Habitually monitoring for potential security threats can trigger a conscious process of deeper investigation, which, if successful, reinforces the habit of monitoring. Monitoring and investigating can also inform subsequent evaluating of the relative risk of threats. Evaluating serves to regulate further monitoring and investigating.

threats can trigger a more deliberate process of investigating those threats. Investigating can reinforce the habit of monitoring through the rewarding experience of discovering a threat, and it can also provide the monitoring system with more information to use in scanning for future threats. Multiple participants said that after they personally identified an instance of some security flaw, they became more vigilant about that flaw in the future.

Participants who mentioned evaluating described it as being informed, in part, by the experience of monitoring and investigating. By continually searching for and identifying potential threats, people who practice monitoring and identification tend to build what one participant described as a mental "database of probabilities" and another called a "pantheon of common security failures." This knowledge helps people to evaluate the relative risk associated with a given threat. As the capacity for evaluating develops, it regulates the attention of more experienced professionals so that they monitor and investigate higher-priority threats and ignore smaller ones. Several participants stated that people who lack the capacity for evaluating tend to "waste energy," to be "worried about the wrong things," or to have an "immature security mindset."

As defined here, the security mindset is a morally neutral process of identifying and evaluating security flaws in systems. Many participants stated that the security mindset could be used by prosocial or malicious actors to attack systems or to defend them. In the cybersecurity industry, it is common to differentiate between "white-hats," who are hackers who explore systems with the consent of their owners, and "gray-" or "black-hats" who do not [58]. Although some participants did indicate they had dabbled in black- and gray-hat activities in the past, most of the sample strongly identified as white-hats.The three-aspect model of the security mindset is also domain-general—in principle, it can apply to any domain of potential security threats. This matches anecdotal descriptions of the security mindset [1] and the reports of our participants, who described experiences with digital systems, physical systems like locked doors, and even systems of social interaction and social engineering.

Finally, the three-aspect model helps to clarify the role of security expertise and technical knowledge for the security mindset. Monitoring relies on knowledge of cues that something in the threat landscape is abnormal or potentially vulnerable. Investigating typically relies on technical knowledge about how systems work. Evaluating relies on knowledge of a history of security flaws and which were high-priority, as well as supporting knowledge about the goals and abilities of attackers. Over time, the processes of monitoring, investigating, and evaluating build up their corresponding sets of knowledge. However, as our participants noted and others have previously argued, knowledge and experience are not synonymous with the security mindset because people must be motivated to use them to proactively seek out new security flaws [1, 6, 17, 19, 31]. The following two sections of this article help to explain this motivation by describing participants' personal beliefs and developmental histories related to the security mindset.

Beliefs associated with the security mindset

Many participants endorsed one or more distinctive beliefs that they described as important to their security mindsets. One outlier participant even claimed that a security mindset is not constituted by the processes of monitoring, investigating, and evaluation at all. Instead, the participant conceptualized a security mindset as a set of beliefs that lead people to employ such processes [18].

One commonly held belief was that the digital, physical, and social worlds are filled with social conventions and abstractions that are provided by authorities to simplify and guide behavior, but that they can be hacked or reimagined with a more granular understanding of the world. For example, one participant described how antivirus software is presented to consumers as a simple kind of shield against attackers, when in reality the interactions between antivirus programs and malware can be far more complex. Another participant described how a locked door can be seen as an abstract object that can only be opened with a key, but is actually just a piece of physical material that is held in place with hinges. A third participant described how many people never reflect on the social conventions between security staff and visitors, when in reality there is nothing stopping one from breaking those conventions. In each case, participants expressed the belief that these abstractions obscure viable and creative courses of action, such as bypassing a firewall, taking the hinges off of a door to open it, or adopting a confident demeanor to walk past security.

Relatedly, several participants expressed the idea that people who are willing to see beyond simple abstractions have power over those who are not, and that this power can be used to cause or prevent harm. One participant used a metaphor sometimes referenced in security, military, and law enforcement circles that there are three kinds of people in the world—"sheep," "wolves," and "sheepdogs" [59]. "Sheep" are people who live happily oblivious to the true nature of the world, while those who do not are either "wolves," who abuse their power to prey on the sheep, or "sheepdogs," who use their power to stop the wolves.

A belief in the existence of "wolves" could lead some to see the world as a fundamentally dangerous place—a worldview that has been studied by psychologists [60–62]. We asked participants if they saw the world as a dangerous place. Their answers varied, but most tended to see the world as somewhat dangerous. However, when speaking about the moral character of humanity, participants were generally positive and expressed the opinion that only a small percentage of people were actively malicious.

Development of the security mindset

We asked participants to describe the origins of their security mindsets. Their responses varied depending on which aspect of the security

mindset they emphasized. We present major themes below. Broadly, participants described their security mindsets as driven primarily by curiosity, the satisfaction of discovery, and a sense of altruism, but they also described distinct origins for each of the three aspects of the security mindset.

In summary, participants emphasized that their capacity for investigating arose from a strong curiosity for how things work and a willingness to question authority. Most participants believed that the seeds for the security mindset were sown in childhood through an interest in investigating. They mentioned a number of formative experiences, including circumstances that allowed free exploration of technical systems and activities that simulate investigative security work.

Monitoring tended to develop as a complement to investigating, or in response to environments that were dangerous or that otherwise strongly rewarded attentiveness to potential security flaws. Some participants suggested that being female or holding some kind of minority status might contribute to a greater capacity for monitoring out of a need for personal safety (though others disagreed), but that social conventions and/or lack of access to resources might make it more difficult for these groups to practice investigating. Finally, evaluating developed later than investigating or monitoring, arose from a need to strategically allocate resources at work, and was described as less inherently enjoyable than the other two aspects.

Development of investigating

Most participants described investigating as an inherently enjoyable process, and almost all of them described *curiosity about how things work* as the single most important personality trait for the development of their capacity for investigating. This is because investigating often comes up empty. Participants that gave a quantitative estimate said that 70–90% of their searches do not lead to a security vulnerability being identified. Instead, participants are often motivated by the desire to simply understand a system. Though they all described enjoying the process of investigating, many participants also described being sensitive to the visceral reward of uncovering a security flaw, using phrases like "dopamine hit," "burst of adrenaline," and "blast of brain chemicals." One participant said that "there is nothing like it":

> But there is no brain chemical endorphin feeling better than going "Oh, my God, I know a thing. I figured it out, I figured the thing out." There's nothing, there's nothing better in my brain at all, like, and that can be triggered not only by cybersecurity but can be triggered by making any kind of connection between two things people don't normally make connections between. (McKayla)

Many participants also described feeling a sense of altruistic pleasure from protecting others. One participant described themselves as "one of the good guys" protecting against "the bad guys," another described feeling mostly driven by "service," a third described finding a vulnerability as feeling like helping a stranger on the street, and a fourth said: "Whether I find a flaw or not, both is a good outcome: if I don't find one that means we're safe, if I do find one that means because of me we will get safer."

Participants also frequently mentioned *a willingness to question authority* as important for investigating [63]. Many participants described a history of testing, questioning, and challenging authority figures such as parents and teachers. Some participants likened this to the security mindset, saying that both involve questioning assumptions, nonconformity, and rule-breaking.

> I always kind of had a problem with authority. Growing up, I was never very… I always told high school teachers that they had to earn respect to get it and they never wanted that. Like, I was always that type of person. Like, I never had a blind acceptance of authority. You know, I would talk back if I felt disrespected, or if I felt singled out. So maybe that plays into it. (Samantha)

In addition to the personality traits described above, many participants described one or more formative experiences that contributed to the development of their interest in investigating. We note two below.

Circumstances which allowed free exploration of technical systems were said to aid in the development of investigating. Many participants described taking toys apart in their childhood to see how they would function. They saw this as a first instance of a curiosity for understanding the underlying mechanisms of things—a curiosity that persisted in adult life and came to fruition in cybersecurity. In the early days of the internet and home computing (when many participants were teenagers), computer and telecommunication systems also had very few enforced rules and consequences. Many participants stated that the freedom to explore and play around in this context was essential to them developing a security mindset.

> The early internet was an ideal place to apply that curiosity. Because unlike the schoolyard or unlike around the house, frequently, that curiosity could, you know, you could see it through to its conclusion. It goes as deep as you had time for, but frequently without a lot of consequences. Which was great, because I think I like a lot of other people from that generation, we just wanted to explore, we wanted to see what was possible. (Jacob)

Activities that simulate investigative security work were also mentioned as formative. These included childhood games and playground rivalries, urban exploration (the hobby of infiltrating and exploring spaces such as sewers, roofs, or boiler rooms), and hacking competitions.

> Well, I think the security mindset arises from a sense of adventure. […] Yeah, this is like around eight or nine years old. […] I kind of had a rivalry with a student at school. […] And we would sort of plan these very elaborate things against each other. Like we would like, try to intercept each other's secret messages. […] It felt very real. I mean, I'm calling them games now. But you know, when we're, when I was younger, this was like, a big deal. […] I remember lying in bed at night for hours, thinking through, okay, what's my next step in this? […] It was just sort of training my mind to think very in depth. Thinking several steps ahead, based on what the adversary might do. […] So I think, something in there, there's something in there I think, fundamental to a security mindset. (George)

In summary, participants described their history of investigating as deeply driven by curiosity about technical systems. They often had support and free opportunities to explore these systems as part of games and personal projects in childhood and young adulthood, and they were willing to challenge authority figures in the process of doing so.

Development of monitoring

For many of our participants, monitoring arose naturally from an existing personal interest in investigating technical systems. The pleasure of investigating simply led these participants to monitor for new opportunities to do it. But many other participants mentioned that *a social environment that values security or security-related behaviors and traits* contributed to the development of their capacity for both

monitoring and investigating. For example, one participant spent extensive time in a hacking club. Another inherited experience from a military family:

> I was raised in a military family. [… Security concerns were] a very normal thing to discuss. It's very normal to be like "Hey, we're going to go get the booth in the corner." Like that was just very normal. And we always knew where dad or grandpa was gonna sit. […] And then as you develop your own sense, and get into that field yourself, you have the ability to also think about those things. (Ash)

For others, monitoring emerged as a means of self-protection in a potentially dangerous or even abusive environment. For example, one participant noted that his military experience trained a quality of situational awareness that translated to cybersecurity. Another believed that growing up in the Soviet Union trained them to monitor for security flaws:

> Anyone who's grown up in the Soviet era has a baseline paranoia about the government listening. […] I already had a proclivity towards it even before I started studying in school. There's a Russian mindset that often shows up, not for everybody obviously, but like "a vulnerability in the system is there to be exploited, and it's the fault of the system if it cannot lock." […] I remember having that kind of socialization, like: systems like shoplifting is yet another system to be hacked, right? (Pseudonym redacted)

Several participants provided personal examples of growing up in abusive or dysfunctional circumstances that led to the cultivation of a capacity for monitoring and/or investigating. One participant reported developing a capacity for monitoring through growing up in a "house full of secrets" related to family abuse. In order to stay safe themselves, they learned to surreptitiously listen in on conversations and access private documents in the house. Another participant described their capacity for monitoring and investigating as developing from the experience of growing up with a mother who had a "narcissistic parenting style":

> So I would try to make sure that you, you know, try to understand her. I was basically, like, I was hacking my mom's emotional states, right? "If I understand what it is that you need to hear from me in order for you to be okay." Right. And then making sure that I followed that. […] To be honest, the security mindset… It wasn't till somebody else said the term that I was like, "Oh, yeah, I guess that is kind of how I do things." […] It was just me growing up. (Pseudonym redacted)

Development of evaluating

According to our participants, the capacity for evaluating developed later than the capacity for monitoring or investigating. Many described going through a phase of believing that, in their words, "everything is leaky" or that "there are holes everywhere"—what one participant called an "immature security mindset"—before updating to a more nuanced worldview that takes relative risk into account:

> I think I initially got better at exploitation […] than I did about having calibrated threat models. And so when you realize how vulnerable everything is that is scary, because everything IS really vulnerable. […] If you have agents that are in your environment, actively exploiting things all the time, then you should be scared or something, right, because there are all of these exploits. But in most scenarios, there are some agents that want to exploit things, but they usually are pretty specific. They usually have specific reasons. And it's not that scary. (Damian)

Unlike monitoring or investigating, evaluating was not described as inherently enjoyable or satisfying, and no participants described any childhood experiences with evaluating—perhaps because it does not involve a concrete and satisfying resolution of finding or exploiting a flaw in a system. Instead, evaluating was primarily described as being instrumentally useful for their personal work or their organization's performance. Accordingly, most participants described developing the capacity for evaluating at the workplace. Typically, this happened organically through on-the-job experience. As one participant put it,

> Sometimes [decisions are] based on just experience, prior experience and ability to think about previous cases and think about cybersecurity holistically. It takes a couple of years of experience in cybersecurity, doing other types of monitoring, triage, etc. So it's time-consuming to build up that mental database of events and security findings, etc., that help you make those decisions on your feet. (Penny)

However, a few participants described deliberately training their evaluating skills by reading case studies and reports of hacks and security flaws:

> So there are larger-scale survey studies that occur annually by various companies, Verizon, for example, where they talk about these techniques that are found in this percentage of incidents, for example. And so you can try to ground your understanding of likelihoods there. (Fabian)

Gender and race

All four of the female participants in the study indicated that the development of the security mindset is a heavily gendered issue. In three out of these four cases, participants proactively brought up gender without the interviewer specifically inquiring about it. However, they described different effects of gender on monitoring and investigating.

Two out of the four female participants stated that they developed a capacity to monitor their environments for their own personal safety. Their reports are consistent with comments from other participants in section 3.3.2 that spending time in unsafe environments contributed to an ability to monitor. However, one female participant was unsure whether monitoring for her personal safety contributed to their work in cybersecurity, and another actively disagreed that there was a relationship between the two.

According to one female participant, women might have fewer opportunities to develop a capacity for investigating because society often discourages them from bending rules, challenging authority, and subverting the intended functions of things:

> Women have this crushed out of them at a really early age: behaving unexpectedly has a much higher penalty for women than it does for men. Your study is missing all of the young women—and especially the young black women—who had this mindset when they were young, but never knew they could develop it, who were told that it was wrong and bad of them to be rude to people, instead of being applauded for thinking unconventionally. (Pseudonym redacted)

One participant suggested that there might be racial differences in the security mindset as well:

> I am a white woman. And I don't know how a lot of my black women friends develop their security mindset. I know fewer of them do than white women. And, white women have a fully developed sense of it less than most white men do. (Pseudonym redacted)

Unfortunately, the sample did not include any participants of Black, Hispanic, or Native American descent. None of the other participants, including the three Asian participants in the sample, gave indication of racial differences related to the development of the security mindset.

Consequences of having a security mindset

Together, monitoring and investigating allowed participants to identify security flaws around them, but in many cases, they became what some participants called an "immature" security mindset—a practice of habitually monitoring and investigating that created stress and conflict in their personal and professional lives. To manage this stress and conflict, some participants pursued distractions, practiced deliberately letting go of their habits, or learned to evaluate the relative severity of security flaws in order to keep them in proper perspective.

Monitoring and investigating help identify security flaws

Existing formal and informal discussion of the security mindset has focused almost exclusively on the supposed advantages of the security mindset for cybersecurity job performance [13–15, 30]. The participants in this study strongly agreed—almost all of them believed that the security mindset improved their performance as a cybersecurity professional.

One participant described it as "probably the core reason why I have been successful in my job." Many others described examples of spotting security vulnerabilities that others overlooked. Several participants in more managerial roles indicated that they look for the security mindset when hiring and they emphasize its value among their existing employees:

> As an executive working in cybersecurity today, I find it very hard to attract, develop and retain talent. So to the extent that your research is able to make it easier to screen for and identify folks that have this so-called security mindset, that's a significant interest to me, both as an American citizen and as an executive working in a cybersecurity function, trying to hire security people. (Jacob)

Unconstrained monitoring and investigating may have negative side effects

Although participants mostly spoke positively of the security mindset, they also mentioned several disadvantages of unconstrained or excessive monitoring and investigating on professional, interpersonal, and intrapersonal levels.

In the workplace, several participants pointed out that cybersecurity professionals who perform a great deal of monitoring and investigating can identify more flaws than an organization has resources to fix. This can create tension between those who identify flaws and those responsible for fixing them, particularly if flaws are low-priority:

> People don't like when people with a security mindset point out vulnerabilities that they think are unlikely to be exploited or like, don't matter, because it makes their job a lot harder. They don't want to have to deal with it. […] And so I think it's often that people are like "security people are so annoying," because they like, bring up these things, and like, these things don't matter anyway. (Damian)

On the interpersonal level, several participants reported that having a strong habit for monitoring and investigating negatively influenced their social life outside of work. Because they were more aware of security vulnerabilities than people without a security mindset, they tended to be more careful, which can be perceived as mistrusting:

> You do tend to get a little bit jaded and overly suspicious of people. And that can affect your interpersonal relationships. Particularly, you know, it's kind of a little harder to make friends when you're so guarded. […] So, my wife hands out her Facebook immediately. Oh my! You've got to go through a lot to get on MY Facebook. Stuff like that. And because of that people perceive it as you're not as warm. (Mick)

Finally, a number of participants emphasized that overzealous and uncontrolled habits of monitoring and investigating can lead to burnout or mental health problems. Constantly monitoring the environment for security flaws can be mentally exhausting and lead to an overly pessimistic worldview:

> You don't need to be a paranoid person to start with, but working in an environment where you've got to worry about every last potential threat vector, I think leads to that burnout […] It's exhausting. And I think that a lot of security people do burn out over time. And I think a primary driver for that burnout is that it really is emotionally and psychologically exhausting to be looking at every situation through the lens of how this thing might fall to pieces. (Jacob)

Methods of regulating monitoring and investigating

Several participants discussed the need to regulate the intensity of monitoring and investigating in order to mitigate the professional, social, and personal downsides described above. They engaged in a variety of strategies. Some aimed to distract themselves from monitoring and investigating through substance use and extreme hobbies.

> The most successful people I know who have this mindset, have some form of recreation, where you must keep your attention totally focused on that form of recreation: motorcycle racing, jujitsu, planes, helicopter skiing, firearms […] If you do my hobbies wrong, you die. […] There is nothing like landing a plane to make you not think about cybersecurity. There is nothing like riding a motorcycle at a 30-degree angle around a mountain curve in the middle of a group ride, to make absolutely sure that you are not thinking about cybersecurity! […] Can you turn it on and off? And the answer I would have is, that is the only way I really can. (Pseudonym redacted)

Others described efforts to "dial back" or "let go" of monitoring and investigating over time:

> I had a friend at my last company… […] He very much had the security mindset. And I observed it in all of his behaviors. But he was a few years older than I was, maybe 10 years older. And over time, he had intentionally dialed it back and modulated that security mindset in order to increase his enjoyment of his life. And the way he articulated it to me was he said, "Look, you know, we look at the world through a peculiar lens, and it reveals to us all these possible things that could go wrong, and we pride ourselves in being able to navigate those situations successfully. But in order to really be grounded, and to be free, and to be happy, we need to let a lot of that go. Moment to moment, day to day." And so I've taken that to heart. (Jacob)

However, the most commonly cited method for regulating monitoring and investigating was to practice evaluating. Many participants suggested that cybersecurity professionals who are able to accurately evaluate the relative risks associated with security flaws are better able to avoid burnout and conflict that might come from an "immature" security mindset:

> So someone who's new to security might see something and think: "Oh, my gosh, this is a critical incident, we've got to… everyone stop what you're doing!" And maybe later, you might say "No, that's not a big deal. We can actually ignore this one, you know, these kinds of things happen every day.." (George)

In particular, multiple participants noted an asymmetry between the perspectives of attackers and defenders in cybersecurity. Attackers succeed if they can exploit a single flaw, so cybersecurity professionals who are trained to find flaws can easily assume that each flaw is an urgent problem. But defenders are often already aware that their systems have many flaws, and their focus is on distributing their limited resources to evaluate and mitigate the flaws that are of greatest concern. Defenders may therefore tend to cultivate more of a capacity for evaluating than attackers, all else equal. Organizational management staff also sometimes have a broader sense of the security priorities of an organization compared to lower-level cybersecurity employees, and so they may have more opportunities to develop evaluating. One participant noted these dynamics in the context of "red" (attacker) and "blue" (defender) professionals working together at an organization:

> People who maybe are on the blue side of things, or management or anything like that, in my experience, I found those people to be considering the risks and you know, weighing it up a lot more. So you kind of have, you know, your pen testers [cybersecurity professionals who focus on identifying flaws] who might get very, very worried. And then you've got your blue team as well […] you know, managers, people who deal with risks day in day out, would consider the risks as well in anything they find and as a result may be less anxious. (Aamir)

Discussion

Theoretical contributions and recommendations for future research

This paper builds on existing work primarily by disentangling the concept of the security mindset using empirical data. Unlike previous treatments of the concept, which viewed it as a unitary entity [1] or proposed a decomposition without supporting empirical data [11], we characterize the security mindset in terms of three distinct but interrelated mental processes. Most participants mentioned all three aspects in their descriptions of their own security mindsets, and they described these aspects as co-occurring and mutually reinforcing.

The three-aspect decomposition of the security mindset suggests a number of directions for future work. Psychology researchers should draw from existing methodologies to develop separate survey measures for monitoring, investigating, and evaluating, investigate their interrelationships and correlations with different aspects of cybersecurity job performance, and eventually use them as targets for evaluating training and other interventions to cultivate a security mindset. Notably, different measures of the security mindset may also be needed for different purposes. For example, measures designed for research and theory development are often optimized for comprehensiveness and psychometric reliability, but they can be impractically time-consuming to administer, and they may be vulnerable to "gaming" or deliberate exploitation [28].

Our research also identified troubling reports of negative effects of an overactive security mindset, including burnout, mental health challenges, and conflicts at work and in personal relationships. Future work should more thoroughly investigate these issues among cybersecurity professionals, the circumstances in which they arise, and effective means of mitigating them. In particular, some of our participants suggested that evaluating cybersecurity flaws helped to regulate the potential negative effects of overactive monitoring and investigating. Researchers could test this hypothesis by assessing the relationships between the negative effects described above and each of the aspects of the security mindset.

Our work also highlights ambiguity in the concept of a "mindset" that has been recognized in psychology but not yet incorporated into the cybersecurity literature. The participants in our study tended to describe monitoring as a mental lens or filter that is passively and habitually applied to experience, while investigating and evaluating were described as more active thought processes. Many participants also shared a common set of beliefs linked to their security mindsets, such as the belief that superficial appearances of systems are not trustworthy, and one participant defined the security mindset in terms of those beliefs.

This range of responses—mindset as filter, active process, or belief—bears a striking resemblance to the range of meanings found in existing psychological research on mindsets [64]. Within social psychology and organizational leadership, mindsets are frequently conceptualized as a *cognitive filter* or frame in which new information is embedded, contextualized, and modified [65, 66]. Within cognitive psychology, a mindset has been conceptualized as *a grouping of cognitive processes* that are activated whenever a certain task is performed [67]. Finally, some scholars conceptualize a mindset as a *set of beliefs about the world* that motivates the adoption of different behaviors and ways of thinking [68, 69].

Future research on the security mindset should draw from different bodies of literature depending on the meaning of "mindset" that they wish to explore. For example, researchers interested in monitoring as a passive cognitive filter could take inspiration from early construct-building efforts related to the global mindset [70]. Those interested in the more active, deliberate aspects of investigating and evaluating could look to treatments of mindset in the cognitive psychological tradition, such as Gollwitzer's work on deliberative vs. implemental mindsets [71]. Finally, though almost all of our participants did not define their security mindsets in terms of beliefs *per se*, researchers might look to scholars such as Dweck [69] to identify beliefs that influence the development of the security mindset.

We also found interesting potential interactions between different aspects of the security mindset and participants' gender backgrounds. Some of our participants suggested that holding a minority status might contribute to a greater capacity for monitoring one's environment for security risks, though others questioned if this generalized to other security domains. Other participants noted that social conventions and/or lack of access to resources might make it more difficult for members of minority groups to practice investigating. These tentative findings illustrate the value of distinguishing monitoring from investigating when considering the security mindset, and should be explored through follow-up research in order to provide the best possible opportunities for all cybersecurity learners.

Participants' descriptions of the security mindset also bear an interesting resemblance to what cognitive psychologists call a model-based mode of learning, in contrast to model-free learning. In model-based learning, a learner first tries to build an accurate model of reality. Then, when faced with a challenge, the learner tries to find a solution by mentally manipulating their imagined model of the world. In contrast, model-free learning is based on trial and error. Here, the learner simply selects actions that have previously worked for themselves or others, without thinking about the underlying mechanism of a system. Future work could examine whether people who self-identify as having a security mindset score higher on tasks that indicate general tendencies toward model-based learning [72].

Our interviews also suggest previously underexplored intersections between the security mindset and organizational structure. As noted above, monitoring, investigating, and evaluating skills appear to be represented to varying degrees among different roles in a cybersecurity organizational hierarchy. Rather than focusing only on individuals, scholars might study the *distributions* of monitoring, investigating, and evaluating across teams that most successfully identify and address cyber threats. For example, some participants in our study raised concerns about friction between management and lower-level cybersecurity staff, who might identify flaws but feel that their concerns are not being taken seriously. This might be understood as an instance of lower-level staff failing to properly evaluate the broader significance of their findings, and/or as managers resisting uncomfortable knowledge that poses a risk to project development timelines. Future research could study these and other organizational dynamics in greater detail.

Finally, in this study, we only interviewed self-identified "white-hat" professionals, not "gray-" or "black-hats" who use their cybersecurity skills without permission of the owners of the systems that they explore. Our study did not investigate the factors that lead people to become black-hats vs. white-hats, or the interaction of those factors with the security mindset. All participants that brought up the issue of the moral nature of the security mindset described it as morally neutral and usable for good or evil. The security mindset was described as a powerful set of mental tools, and some could be inspired to practice caution and protect the vulnerable, while others could be tempted to cause harm. Future research into the security mindset should investigate how to cultivate the conditions in which security mindsets are most likely to be used ethically.

Implications for cybersecurity education, training, and self-directed learning

Can the security mindset be developed? Popular discussions of the security mindset have often considered the extent to which it is or is not trainable [1]. As an initial qualitative investigation, this study does not provide conclusive evidence that the security mindset is trainable, but it suggests potential for significant environmental influences. For many of our participants, monitoring and investigating functioned together as a set of satisfying mental habits that did not always exist, but were driven by curiosity and rewarded by discovery. Participants described developing the capacity for monitoring and investigating through active, exploratory, inquiry-based learning, often via games, simulations, and other supportive social environments in which they could cultivate and indulge their curiosity. Reverse causality and interaction effects are still entirely possible; e.g. people with a predisposition to be curious about mechanical systems may seek out and disproportionately benefit from opportunities to learn about those systems. However, the mechanisms of habit and reward that participants described at the core of the security mindset are universal in humans and non-human animals. Just as virtually all people have the capacity to build strength through exercise, they also have the capacity to build habits through practice and reward [73]. Insofar as the security mindset is composed of habits, it should be at least somewhat trainable.

Educators and trainers should also note that our participants described their security mindsets as being largely intrinsically motivated. Motivation for an activity can be conceptualized on a continuum from more intrinsic (driven by internal rewards inherent to the activity itself) to more extrinsic (driven by external rewards) [74]. Our participants tended to emphasize intrinsic rewards of the security mindset like curiosity, the satisfaction of discovery, and taking pride in their work, and they deemphasized or even criticized the use of external rewards and punishments.

Intrinsic motivation toward an activity is most likely to develop in environments where learners feel a sense of autonomy to choose their own pursuits, a sense of competency in the domain in question, and a feeling of connection and relatedness to other learners like them [75, 76]. Thus, to support intrinsic motivation, educators and trainers should attempt to find or create learning environments in which learners can develop the skills and motivation to exercise the security mindset by freely exploring, discovering, and investigating security challenges that are accessible at their current level of skill. These learning environments should provide a social community that celebrates tinkering, hacking, bending rules, and asking questions, and they should link the rewards of discovery to outcomes that the learner intrinsically values, whether that is pride in one's work, a deeper understanding of the workings of a system, or even an opportunity to play a fun harmless prank on a friend. Indeed, a number of our participants described developing their own security mindsets through similar circumstances. Makerspaces could serve as a useful source of inspiration [77, 78].

While a full review of inequities in cybersecurity education and practice is outside of the scope of this article [79, 80], our research highlights one particular dimension of inequity that deserves further investigation. Our study participants described developing a security mindset in part through free exploration, questioning authority, and some degree of bending and breaking accepted rules of conduct. But learners from marginalized backgrounds often face societal pressure to conform to strict standards of appropriate behavior and experience heavy-handed punishment for disobedience [81, 82]. Some of these learners might feel unsafe or uncomfortable engaging in cybersecurity learning activities that are associated with rule-breaking and crime. Future work should investigate the extent to which this dynamic exists and design correctives to support a wider range of cybersecurity learners.

Finally, educators and trainers should consider deliberately developing the evaluating aspect of the security mindset. Our participants indicated that, to some extent, evaluating simply developed with experience over time. However, some participants also claimed that the development of evaluating could be accelerated by reading case studies and reports of real-world security flaws, by conversing with colleagues about high-priority targets and commonly-used attack routes, and sometimes even by speaking with non-security personnel. Educators could potentially adapt this advice for training evaluating abilities among penetration testers and other investigating-focused cybersecurity professionals.

Implications for cybersecurity recruitment

Employers and recruiters seeking to identify job candidates with a security mindset have a number of options available, though more work is needed to evaluate their practical feasibility. First, as described above, curiosity about technical systems appears to be a core driver of the investigating aspect of the security mindset, and it was the single most frequently used code in our study. To the extent possible, employers and recruiters should try to learn about candidates' genuine curiosity about technical systems. It may be possible to develop survey measures or behavioral assessments of candidates' curiosity about technical systems, but a great deal of care is needed to ensure that such assessments are not "gamed" or exploited by applicants (an ironic fate for a measure of the security mindset!).

Employers and recruiters might also ask job candidates who have experience in monitoring and investigating about their ability to eval-

uate the relative priority of different security flaws. For example, they might combine a bug-bounty performance test with a task of explaining the relative risk of different bugs, given different sets of background assumptions. They might also ask candidates for their preferred sources of information about the relative risks of security flaws, or they might inquire about the candidate's interactions with CISOs or other staff who are more likely to hold an evaluating-heavy role.

Implications for cybersecurity management

Our research suggests that managers of cybersecurity teams may, at least in some cases, be particularly likely to have experience with the "evaluating" aspect of the security mindset. In our sample, monitoring and investigating were emphasized by participants from a variety of different roles, but evaluating was particularly emphasized by participants working in "Govern & Support" and "Design & Develop" roles, such as CISOs and cybersecurity managers. Evaluating also appeared to help mitigate some of the potential negative consequences of constant monitoring and investigating, such as mental health challenges and misaligned work priorities.

These findings suggest that managers and other senior staff should monitor cybersecurity employees for burnout and other mental health issues, provide mental health support resources as needed, and connect employees with senior mentors and contextual information about organizational goals in order to help them develop the skill of evaluating security flaws in context. By doing so, they might help inform better frontline risk prioritization, improve team communication, and reduce potential risks of burnout.

Implications for policymakers

There are many efforts across US government agencies to build a more capable cybersecurity workforce [83]. While our results are only based on an initial study of 21 cybersecurity experts, they suggest several initial implications for policymakers:

- Fund the creation of learning environments that support the intrinsic motivation to responsibly practice monitoring, investigating, and evaluating in cyber contexts, inspired by makerspaces and similar environments. Make sure that all learners have access to these environments and feel permitted to explore them without stigma—particularly women and members of minority groups who may face particular social pressure to be perceived as rule-abiding and trustworthy.
- Fund research to operationalize metrics of each aspect of a security mindset, and to test for their relationships with cybersecurity performance outcomes before exploring their potential usage for recruitment.
- Update the DHS Cybersecurity Workforce Development Toolkit [84] to include information about assessing and mitigating employee mental health concerns, particularly among staff such as penetration testers that may practice extensive monitoring and investigating.

Limitations

This study set out to explore the security mindset as a concept by exploring the perspectives of 21 cybersecurity professionals. Although the sample size of this study is moderately large for a qualitative study [85], it is still small and focused on the USA. As such, our claims are preliminary and readers should take caution in generalizing from our findings. It is also difficult to draw strong conclusions about subgroups included in our sample, such as women or those working in the different roles of the CCCS' Workforce Development and Curriculum Guide. Importantly, Black, Latino, and Hispanic participants were also missing in the sample, and may provide a unique perspective not captured by this study.

Our study focused on the perspectives of cybersecurity professionals who already self-identify as having a security mindset based on the minimal description that we formulated from past literature ("the tendency to look for and think about security flaws in the systems around oneself, even when one is not directly instructed to do so"). Selecting participants who fit this description allowed us to focus on our construct of interest, rather than other meanings of the term "security mindset" that participants might use. Future work could use a more open-ended recruitment approach to investigate these other meanings. In addition, it is theoretically possible that some potential participants mis-identified themselves and thus mistakenly included or excluded themselves from the study. However, we found that our participants' responses were internally coherent and could be grouped into three distinct aspects. In the future, these aspects could be used to develop metrics that can rely less on self-report.

As we conducted interviews, we also sometimes shared some of our evolving impressions of the security mindset with participants to check if they resonated and to prompt further discussion. We only did this toward the end of the interviews to make sure that we did not color participants' responses. This technique has been recommended for "ensuring accurate representation of participants' perspectives or experiences" [86], which seemed particularly important as neither interviewer had a security background. Sharing initial impressions has also been recommended for qualitative research involving early-stage definitions of a construct of interest [53, 87, 88].

However, relying on participants to self-identify and offering them our initial impressions also inevitably creates some potential for social desirability bias [89]. For example, participants might have overstated the utility of having a security mindset, or understated its drawbacks, in order to more favorably present themselves in interviews. In order to mitigate these risks, we used established interview techniques to guard against social desirability bias, such as not attributing ideas to ourselves ("What do you think of this idea?" vs. "What do you think of our idea?"), prefacing our questions to assure participants that all answers are acceptable, and asking for follow-up information [90]. Future work could further mitigate risks of bias by seeking out the perspectives of a wider range of cybersecurity professionals, including those who do not personally identify as having a security mindset, and by using research designs that minimize two-way sharing.

Conclusion

The globe is currently facing a cybersecurity "skills gap" [12]. The security mindset is often discussed in cybersecurity circles as an important, elusive, and possibly even untrainable quality of the best cybersecurity professionals [1], but empirical research on the security mindset is sparse.

We conducted interviews with 21 cybersecurity professionals who self-identified as having a security mindset in order to understand more about how the security mindset operates, where it comes from, and what effects it has on participants' personal and professional lives. We found that our participants described the security mindset in terms of three interlocking habitual mental processes: un-

conscious monitoring for anomalies and potential threats, deliberate investigating of systems to identify security flaws, and evaluating the relative risks of those flaws once discovered. We also identified several common traits and formative experiences of those with a security mindset, and we heard from participants that the security mindset was often enjoyable and professionally valuable, but that it could cause stress, conflict, and burnout if not held in check.

In order to protect against future attacks and build a more resilient digital infrastructure, we need to understand what makes a great cybersecurity expert. Future work should replicate, refine, and operationalize our findings in the field in order to cultivate a generation of cybersecurity professionals who can successfully monitor, investigate, and evaluate potential threats in a healthy, well-balanced, and ethically responsible manner.

Supplementary data

Supplementary data is available at *Cybersecurity Journal* online.

Acknowledgements

The authors would like to thank Gerjo Kok, Rosanna Guadagno, Tom Berson, Kathryn Brink, our study participants, and our anonymous reviewers for their valuable feedback on this project.

Conflict of interest statement

The authors declare no conflicts of interest in regard to this article.

Funding

This work was supported by the Open Philanthropy Project.

Author contributions

Koen Schoenmakers (Conceptualization, Formal analysis, Investigation, Methodology, Project administration, Writing – original draft, Writing – review & editing), Daniel Greene (Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Software, Supervision, Visualization, Writing – original draft, Writing – review & editing), Sarah Stutterheim (Supervision, Writing – original draft, Writing – review & editing), Herbert Lin (Conceptualization, Methodology, Supervision, Writing – review & editing), and Megan J. Palmer (Conceptualization, Funding acquisition, Methodology, Project administration, Resources, Software, Supervision, Writing – original draft, Writing – review & editing).

References

1. Schneier B. The security mindset – Schneier on security. *Schneier on Security* 2008.
2. Naden C. The cybersecurity skills gap. 2021. www.iso.org (8 January 2022, date last accessed).
3. Vogel R. Closing the cybersecurity skills gap. *Salus Journal* 2016;**4**:32.
4. Rosso C. The real-world impact of the global cybersecurity workforce gap on cyber defenders. *Dark Reading* 2021.
5. Morgan S. Cybersecurity Jobs Report 2018–2021. *Cybersecurity Ventures* 2021:1–5.
6. Joint Task Force on Cybersecurity Education. *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. New York, NY: Association for Computing Machinery, 2017.
7. Burrell DN. An Exploration of the Cybersecurity Workforce Shortage. *Int J Hyperconnect Internet Things* 2018;**2**:29–41.
8. Peslak A, Hunsinger DS. What is cybersecurity and what cybersecurity skills are employers seeking? *IIS* 2019;**2**:67–72 10.48009/2_iis_2019_62-72
9. Emsi. Build (Don't Buy): A Skills-Based Strategy to Solve the Cybersecurity Talent Shortage. 2020. https://lightcast.io/resources/research/build-don-t-buy (6 January 2022, date last accessed).
10. Petersen R, Santos D, Smith MC *et al.* Workforce Framework for Cybersecurity (NICE Framework).https://doi.org/10.6028/NIST.SP.800-181r1 (6 January 2022, date last accessed).
11. Padmos A. Against mindset. *Proceedings of the New Security Paradigms Workshop on – NSPW '18*, 2018. p. 1–16.
12. ISC2. $(ISC)^2$ 2020 Cybersecurity Workforce Study (English). 2020. www.isc2.org (6 January 2022, date last accessed).
13. Tripwire. The Security Mindset: The Key to Success in the Security Field. https://www.tripwire.com/state-of-security/the-security-mindset-the-key-to-success-in-the-security-field (6 January 2022, date last accessed).
14. O'Toole B. How to build a security mindset. https://www.linkedin.com/pulse/how-build-security-mindset-brian-o-toole/ (6 January 2022, date last accessed).
15. Conti G, Caroland J. Embracing the Kobayashi Maru: why you should teach your students to cheat. *IEEE Secur Priv* 2011;**9**:48–51.
16. International Computer Science Institute. Lesson 1 – The Security Mindset: Cybersecurity through Threat Modeling. https://teachingsecurity.org/lesson-1-the-security-mindset/ (8 January 2022, date last accessed)
17. Cappos J, Weiss R. Teaching the security mindset with reference monitors. *Proceedings of the 45th ACM Technical Symposium on Computer science education – SIGCSE '14*, 2014. p. 523–8.
18. Dutton WH. Fostering a cyber security mindset. *Internet Policy Rev* 2017;**6**:1–14.
19. Bonver E, Cohen M. Developing and retaining a security testing mindset. *IEEE Secur Priv* 2008;**6**:82–5.
20. Hooshangi S, Weiss R, Cappos J. Can the security mindset make students better testers? *Proceedings of the 46th ACM Technical Symposium on Computer Science Education – SIGCSE '15*, 2015. p. 404–9.
21. Pournaghshband V. Teaching the security mindset to CS1 students. *Proceeding of the 44th ACM technical symposium on Computer science education – SIGCSE '13*, 2013. p. 1–6.
22. Brown KW, Ryan RM, Creswell JD. Mindfulness: theoretical foundations and evidence for its salutary effects. *Psychol Inq* 2007;**18**:211–37.
23. Beilock SL, Carr TH. On the fragility of skilled performance: what governs choking under pressure? *J Exp Psychol Gen* 2001;**130**:701–25.
24. Walton GM, Cohen GL. A question of belonging: race, social fit, and achievement. *J Pers Soc Psychol* 2007;**92**:82.
25. Creswell JD. Mindfulness interventions. *Annu Rev Psychol* 2017;**68**:491–516.
26. Ramirez G, Beilock SL. Writing about testing worries boosts exam performance in the classroom. *Science* 2011;**331**:211–3.
27. Walton GM, Brady ST. The social-belonging intervention. In: Walton GM, Crum AJ (eds.), *Handbook of Wise Interventions: How Social-Psychological Insights can Help Solve Problems*. New York, NY: The Guilford Press, 2020, 36–62.
28. Yeager D, Bryk A, Muhich J. *et al. Practical Measurement*. California, CA: Carnegie Foundation for the Advancement of Teaching. 2013.
29. Walton GM, Crum AJ. *Handbook of Wise Interventions*. New York, NY: The Guilford Press, 2020.
30. Nassiokas T. Security mindset – What is it? Why is it important? What does Bruce Schneier think?. https://www.linkedin.com/pulse/security-mindset-what-why-important-does-bruce-think-theo-nassiokas/ (8 January 2022, date last accessed).
31. Potter B, McGraw G. Software security testing. *IEEE Secur Priv* 2004;**2**:81–5.
32. Severance C. Bruce Schneier: the security mindset. *Computer* 2016;**49**:7–8.

33. Haney JM, Theofanos M, Acar Y. *et al.* "We make it a big deal in the company": Security mindsets in organizations that develop cryptographic products.. *SOUPS '18: Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*, 2018, p. 357–73.
34. Smith J, Theisen C, Barik T. A case study of software security red teams at Microsoft. *2020 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*. Dunedin, New Zealand: IEEE, 2020, p. 1–10.
35. Sommestad T, Karlzén H, Hallberg J. A meta-analysis of studies on protection motivation theory and information security behaviour. *Int J Inf Secur Priv* 2015;**9**:26–46.
36. Briggs P, Jeske D, Coventry L. Behavior change interventions for cybersecurity. In: Little L, Sillence E, Joinson A (eds.), *Behavior Change Research and Theory*. United Kingdom: Elsevier, 2017, 115–36.
37. Kam H-J, Menard P, Ormond D. *et al.* Cultivating cybersecurity learning: an integration of self-determination and flow. *Comput Secur* 2020;**96**:101875.
38. Kam H, Ormond DK, Menard P. *et al.* That's interesting: an examination of interest theory and self-determination in organisational cybersecurity training. *Inf Syst J* 2021;**32**:888–926.
39. Reeves A, Calic D, Delfabbro P. "Get a red-hot poker and open up my eyes, it's so boring"[1]: employee perceptions of cybersecurity training. *Comput Secur* 2021;**106**:102281.
40. Markus HR. What moves people to action? Culture and motivation. *Curr Opin Psychol* 2016;**8**:161–6.
41. Henrich J. Culture and social behavior. *Curr Opin Behav Sci* 2015;**3**:84–9.
42. AlHogail A, Mirza A. Information security culture: a definition and a literature review. *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*. Hammamet, Tunisia: IEEE, 2014, 1–7.
43. da Veiga A, Astakhova LV, Botha A. *et al.* Defining organisational information security culture—perspectives from academia and industry. *Comput Secur* 2020;**92**:101713.
44. Nel F, Drevin L. Key elements of an information security culture in organisations. *ICS* 2019;**27**:146–64.
45. Alshaikh M. Developing cybersecurity culture to influence employee behavior: a practice perspective. *Comput Secur* 2020;**98**:102003.
46. Xie J, Lipford HR, Chu B. Why do programmers make security errors? *2011 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*. Pittsburgh, PA: IEEE, 2011, 161–4.
47. Xiao S, Witschey J, Murphy-Hill E. Social influences on secure development tool adoption: why security tools spread. *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*. Baltimore Maryland, MA: ACM, 2014, p. 1095–106.
48. Votipka D, Abrokwa D, Mazurek ML. Building and validating a scale for secure software development self-efficacy. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Honolulu, HI: ACM, 2020, p. 1–20.
49. Vance A, Siponen M, Pahnila S. Motivating IS security compliance: insights from habit and protection motivation theory. *Inf Manag* 2012;**49**:190–8.
50. Chen Y, Galletta DF, Lowry PB. *et al.* Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. *Inf Syst Res* 2021;**32**:1043–65.
51. Sjoberg L. Worry and risk perception. *Risk Anal* 1998;**18**:85–93.
52. Rinner MTB, Gloster AT. Assessing worry: an overview. In: Gerlach AL, Gloster AT (eds.). *Generalized Anxiety Disorder and Worrying*. 1st ed. New Jersey: Wiley, 2020, 9–23.
53. Younas A, Porr C. A step-by-step approach to developing scales for survey research. *Nurse Res* 2018;**26**:14–9.
54. Canadian Centre for Cyber Security. *Workforce Development and Curriculum Guide: A Role-Based Guide for Hiring Managers, Education, and Training Providers*. Government of Canada, 2020.
55. Braun V, Clarke V, Hayfield N. *et al.* Thematic analysis. In: Liamputtong P (ed.), *Handbook of Research Methods in Health Social Sciences*. Singapore: Springer, 2019, 843–60.
56. Braun V, Clarke V. Using thematic analysis in psychology. *Qual Res Psychol* 2006;**3**:77–101.
57. McDonald N, Schoenebeck S, Forte A. Reliability and inter-rater reliability in qualitative research: norms and guidelines for CSCW and HCI practice. *Proc ACM Hum-Comput Interact* 2019;**3**:1–23.
58. Tanczer LM. 50 shades of hacking: how IT and cybersecurity industry actors perceive good, bad, and former hackers. *Contemp Secur Policy* 2019;**41**:108–28.
59. Grossman LtColD. *On Combat: The Psychology and Physiology of Deadly Conflict in War and in Peace*. Illinois: PPCT Research Publications, 2012.
60. Stroebe W, Leander NP, Kruglanski AW. Is it a dangerous world out there? The motivational bases of American gun ownership. *Personal Soc Psychol Bull* 2017;**43**:1071–85.
61. Cook CL, Li YJ, Newell SM. *et al.* The world is a scary place: individual differences in belief in a dangerous world predict specific intergroup prejudices. *Group Process Intergroup Relat* 2016;**21**:584–96. https://doi.org/101177/1368430216670024.
62. Blum SC, Silver RC, Poulin MJ. Perceiving risk in a dangerous world: associations between life experiences and risk perceptions. *Soc Cogn* 2014;**32**:297–314.
63. Caloyannides MA. Enhancing security: not for the conformist. *IEEE Secur Privacy* 2004;**2**:87–8.
64. French RP, II. The fuzziness of mindsets. *Int J Organ Anal* 2016;**24**:673–91.
65. Gupta AK, Govindarajan V. Cultivating a global mindset. *Acad Manag Perspect* 2002;**16**:116–26.
66. Rhinesmith SH. Global mindsets for global managers. *Train Dev* 1992;**46**:63–9.
67. Gollwitzer PM, Bayer U. Deliberative versus implemental mindsets in the control of action. In: Chaiken S, Trope Y (eds.), *Dual-Process Theories in Social Psychology*. New York, NY: The Guilford Press, 1999, 403–22.
68. Brooks R, Brooks S, Goldstein S. The power of mindsets: nurturing engagement, motivation, and resilience in students. In: *Handbook of Research on Student Engagement*. New York: Springer, 2012, 541–62.
69. Dweck C. *Mindset : Changing the Way You Think to Fulfil Your Potential*. London: Constable & Robinson, 2017,
70. Perlmutter HV. The Tortuous Evolution of the Multinational Corporation. *Practicing Manager* 1969;**17**:13–8.
71. Gollwitzer PM. Action phases and mind-sets. In: Higgins ET, Sorrentino RM (eds.), *Handbook of Motivation and Cognition, Volume 2: Foundations of Social Behavior*. New York, NY: The Guilford Press, 1990, 53–92.
72. Kool W, Cushman FA, Gershman SJ. When does model-based control pay off? *PLoS Comput Biol* 2016;**12**:e1005090.
73. Wood W, Rünger D. Psychology of habit. *Annu Rev Psychol* 2016;**67**:289–314.
74. Deci EL, Ryan RM. Self-determination theory: a macrotheory of human motivation, development, and health. *Can Psychol/Psychologie Canadienne* 2008;**49**:182.
75. Niemiec CP, Ryan RM. Autonomy, competence, and relatedness in the classroom: applying self-determination theory to educational practice. *Theory Res Educ* 2009;**7**:133–44.
76. Kusurkar RA, Croiset G, Ten Cate TJ. Twelve tips to stimulate intrinsic motivation in students through autonomy-supportive classroom teaching derived from self-determination theory. *Med Teach* 2012;**33**:978–82. https://doi.org/103109/0142159×2011599896.
77. Konstantinou D, Parmaxi A, Zaphiris P. Mapping research directions on makerspaces in education. *Educ Media Int* 2021;**58**:223–47.
78. Marsh J, Wood E, Chesworth L. *et al.* Makerspaces in early childhood education: principles of pedagogy and practice. *Mind Cult Act* 2019;**26**:221–33.

79. Peacock D, Irons A. Gender inequality in cybersecurity: exploring the gender gap in opportunities and progression. *GST* 2017;**9**:25–44.
80. Esin JO. A call for concern: the unbalanced representation of minorities and women in cybersecurity profession. *J Women Minor Technol* 2020;**2**.1–11
81. Skiba RJ, Michael RS, Nardo AC. *et al.* The color of discipline: sources of racial and gender disproportionality in school punishment. *Urban Rev* 2002;**34**:317–42.
82. Morris EW, Perry BL. Girls behaving badly? Race, gender, and subjective evaluation in the discipline of African American girls. *Sociol Educ* 2017;**90**:127–48.
83. Cybersecurity & Infrastructure Security Agency. Cybersecurity Workforce Development Resources. 2020. https://niccs.cisa.gov/workforce-development (8 January 2022, date last accessed).
84. National Initiative for Cybersecurity Careers and Studies. Cybersecurity Workforce Development Toolkit. https://nistcsf.com/wp-content/uploads/2019/01/DHS-cybersecurity_workforce_development_toolkit.pdf (8 January 2022, date last accessed).
85. Boddy CR. Sample size for qualitative research. *Qual Mark Res Int J* 2016;**19**:426–432.
86. Thomas DR. Feedback from research participants: are member checks useful in qualitative research? *Qual Res Psychol* 2017;**14**:23–41.
87. Waltz CF, Strickland O, Lenz ER. *Measurement in Nursing and Health Research*. 5th edn. New York, NY: Springer Publishing Company, 2017.
88. Miller VA, Reynolds WW, Ittenbach RF. *et al.* Challenges in measuring a new construct: perception of voluntariness for research and treatment decision making. *J Empir Res Hum Res Ethics* 2009;**4**:21–31.
89. Krumpal I. Determinants of social desirability bias in sensitive surveys: a literature review. *Qual Quant* 2013;**47**:2025–47.
90. Bergen N, Labonté R. "Everything Is Perfect, and We Have No Problems": detecting and limiting social desirability bias in qualitative research. *Qual Health Res* 2020;**30**:783–92.