Article

PSYCHOLOGY
LEARNING & TEACHING

Psychology Learning & Teaching
1–17
© The Author(s) 2023
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/14757257231214612
journals.sagepub.com/home/plj
Sage

An Exploration of the Awareness and Attitudes of Psychology Students Regarding Their Psychological Literacy for Working in the Cybersecurity Industry

Jacqui Taylor
Bournemouth University, UK

Monica Whitty
Monash University, Australia

Abstract

We propose that psychology graduates are uniquely placed to work in the cybersecurity industry due to their understanding of human behavior and the possession of skills needed to address cybersecurity issues. However, there are challenges in attracting psychology graduates to the cybersecurity industry as they may not be fully aware of how skills developed in a psychology degree can be applied to a cybersecurity career. This small-scale evaluation explored psychology students' understanding of what working in cybersecurity entailed and what psychology skills and knowledge (their psychological literacies) they thought were needed for working in psychology and cybersecurity roles. Undergraduate psychology students ($N = 66$) answered two open-ended questions about skills needed to work in cybersecurity and then judged the importance of nine psychological literacy items for working in cybersecurity and psychology. A content analysis revealed that students recognized not just the technical aspects of cybersecurity work but also aspects relating to human behavior. Seven of the nine psychological literacy items were perceived as significantly more important for working in psychology than cybersecurity. This study is the first to link psychological literacy to working in cybersecurity. The implications of the results are discussed in terms of supporting students to recognize their psychological literacies for cybersecurity careers and suggestions are made for awareness-raising initiatives.

Corresponding author:
Jacqui Taylor, Department of Psychology, Bournemouth University, Faculty of Science and Technology, Talbot Campus, Fern Barrow, Poole BH12 5BB, UK.
Email: jtaylor@bournemouth.ac.uk

Keywords

Cybersecurity, psychological literacy, employability, careers, human factors, social engineering

A psychology degree provides excellent training for a wide variety of careers outside of being a psychologist. Over the last 20 years, several initiatives and research publications have highlighted the need to enable opportunities for psychology students to recognize and apply their psychology understanding and skills to other contexts, locally, nationally, and globally. This has been termed psychological literacy (PL) and was defined by McGovern et al. (2010) as including nine elements (these are detailed within the “Method” section). Since McGovern’s definition and conceptualization, several psychology academics have suggested that PL should be a core principle in the design and operation of psychology undergraduate courses (e.g., Cranney et al., 2022). Although many national organizations (e.g., QAA, 2023) and higher education institutions have taken on this recommendation, there have been some critics. For example, Murdoch (2016) argues that only two of the nine elements defined by McGovern et al. (2010) are exclusively psychological and that seven of the elements (such as critical thinking or acting ethically) are desirable goals for educators across many other disciplines.

The concept of PL has recently been applied to employability within articles discussing the concept of “psychology workforce literacy.” This is defined by Spencer (2021) as, “the ability to articulate the ways in which the knowledge and skills acquired through the psychology major are applicable to diverse occupational domains” (p. 409). Spencer (2021) proposes that psychology academics need to change their way of thinking to consider the role that instructors play in career mentoring, and they propose a comprehensive model that can be incorporated into the undergraduate psychology curriculum. Machin and Gasson (2022) illustrated many examples of how students can apply their psychology understanding and skills in a variety of careers, including those outside of “professional psychology.” Machin, Machin, Jeffries, and Hoare (2022) included chapters in their book that cover careers in clinical psychology; counseling; social psychology; developmental and educational psychology; neuroscience; industrial, work, and organizational psychology; legal psychology; sport psychology; environmental psychology; public health and community psychology; and military psychology. Notable by their absence in this book are careers in information systems, human factors, computing, forensics, and cybersecurity.

Cybersecurity is a frequently used term when referring to the security of information systems or of the safety of people online. However, although some definitions exist many are uninformative or do not adequately cover the multidimensionality of the term. In an attempt to address this, Craigen, Diakun-Thibault, and Purse (2014) conducted a literature review and held discussions with a diverse group of stakeholders including practitioners and academics in cybersecurity. They define the term as, “Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights” (p. 13). According to industry sources (Esentire, 2023), global cybersecurity job vacancies grew by 350%, between 2013 and 2021 from 1 to 3.5 million and many of these positions remain unfilled. The cybersecurity industry has initiated many efforts to attract talented individuals and to deal with burnout, however, the predictions are that the disparity between demand and supply will continue until at least 2025. At the same time, the cost of damages resulting from cybercrime continues to escalate and it is expected to reach $10.5 trillion by 2025 (Esentire, 2023).

Understanding the role of people is central in cybersecurity, including how people may enhance security, how cybercriminals impact technology users, and the role of humans in weakening the defenses set up to protect them. Cybersecurity specialists, for instance, are required to make quick decisions under stressful circumstances, communicating effectively with a range of technical and nontechnical stakeholders (Department for Digital, Culture, Media and Sport, 2022). They must also implement organizational change and develop policies to deter and prevent insider attacks (Whitty, 2021). Understanding human behavior and how individuals might be tricked and persuaded to respond to scams is another essential skill if successful educational and training programs are to be developed to protect organizations and societies (Goh, 2021). Arguably, therefore, psychology graduates are uniquely placed to work in the cybersecurity industry where they can apply their PL in this rapidly expanding job market. However, there are many potential challenges in attracting psychology graduates to work in cybersecurity. This review will identify how PLs can help understand and predict the targets of attacks, identify the perpetrators of cybersecurity attacks, and to suggest ways to defend against these attacks. The review will then discuss the current so-called "cybersecurity skills gap" and identify ways in which psychology skills can be applied within the cybersecurity field.

Applying Psychology Knowledge to Cybersecurity

It has been frequently commented that humans are the weakest link in cybersecurity (Goh, 2021). Arguably, this is an unhelpful phrase, given that due to the failings of technology to protect people, humans must step up and provide the last line of defense. Given this, understanding human psychology is essential to developing effective policies and behaviors to protect citizens and organizations. A key PL that graduates possess is their discipline-specific knowledge of a wide variety of areas in psychology. These areas are often prescribed by national bodies to be covered in psychology degrees, for example, the QAA in the United Kingdom (QAA, 2023). The areas usually covered include cognitive psychology, social psychology, biological psychology, developmental psychology, and individual differences. We shall identify in this section how the literacy "knowledge of psychology" identified by McGovern et al. (2010) can be applied to understand three groups of people involved in cybersecurity: the targets of cyber-attacks (e.g., employees and computer users), the attackers who can be individuals or groups of people (e.g., hackers and intelligence agencies), and the defenders against attacks (e.g., Cyber Security Incident Response Teams).

The Targets of Cyber-Attacks

Cyber-attack targets may include potential scam victims, those tricked into believing untruths, and victims of online harassment and stalking. Susceptibility to scams is associated with many psychological factors, including personality, attitudes and beliefs, employment of heuristics, and online behaviors (Whitty, 2019; Williams, Beardmore, & Joinson, 2017). An understanding of the user's decision-making processes can help to prevent a security compromise; for example, it is important to understand the role of cognitive biases and heuristics, and cognitive load (Andrade & Yoo, 2019). Psychological individual differences have been studied to understand susceptibility to being deceived online. For example, Rajagulasingam and Taylor (2022) studied the role of impulsivity, the need for cognition, and self-control in the correct detection of phishing. Similarly, Whitty (2019) found that those who were less impulsive, those who took their time at a task, and people who were more likely to consider future consequences were more accurate in identifying scams. Personality has been related to susceptibility to being deceived by social media scams such as catfishing and identity theft. For example, Proudfoot et al. (2018) related the way that individuals differed in their desire for privacy versus their desire for impression management when interacting via social media to their susceptibility to being "scammed." Beliefs may also play an important role, for example, Buchanan and Whitty (2014) found that those with more idealized romantic beliefs were more likely to be defrauded by a romance scam.

The Attackers

In addition to understanding the victims, psychological understanding can also be applied to understand the perpetrators of cybersecurity attacks. The people involved in cyber-attacks and privacy breaches might be working alone (e.g., "script kiddies," "hackers," and insiders) or they may work in a group which can range from small criminal gangs, organized criminals, or intelligence agencies from nation-states. Attempts to illegally gain personal data often rely on social engineering techniques to trick people into clicking a link within a phishing email or offering up information to someone they falsely believe to be a trustworthy source. Organized criminals share knowledge and work collectively to defraud victims out of money (Whitty, 2018). Of further interest is research by Thackray et al. (2017), which found that hackers hold a strong social identity and are motivated by prestige, financial gains, revenge, ideology, and recreation. In other work, psychologists have contributed to an understanding of criminal behavior by identifying the use of profiling of targets by adversaries, for example, in terms of age or social media platform use (Shappie et al., 2020). This information has enabled defenders against attacks to develop education programs specifically for those likely to be targeted (such as older adults or users of certain social media platforms).

The Defenders Against Attacks

Psychology has been applied to inform effective behavior change training programs to improve cybersecurity behavior and practices within organizations. For example, Taylor, McAlaney, Foster, Bello, Maurushat, and Dale (2020) draw on psychological concepts related to teaching and learning to illustrate how cybersecurity training can be effectively created and delivered and the understanding of this material assessed. They highlight the application of cognitive learning theories to develop spaced learning to enhance understanding and they use scenario-based examples to assess likely behavior change. Research from social psychology has contributed to understanding the social influences and attitude change mechanisms involved in encouraging cybersecure behavior (McAlaney et al., 2016). Importantly, these programs acknowledge that "knowing" about cyber risks is not sufficient. Notably, these programs have been used in training cybersecurity professionals and awareness-raising for employees. For example, one common way that employees can be exploited by social engineers is when they over-share information when using social media and there are also organizational risks posed by employees using social media at work.

Applying Psychology Skills to Cybersecurity

Commercial organizations and national governments agree that there is a need for graduates with transferable skills to work in the field of cybersecurity. For example, based on survey and interview data the Department for Digital, Culture, Media and Sport (DCMS, 2022) in the United Kingdom produced a report "A Cyber Security Sectoral Analysis" which highlights what they term as "complementary" or "soft" skills needed for employees working in the field of cybersecurity. In their report, they define these complementary or soft skills as including, "communication, leadership, management, and sales and marketing skills, as well as the ability to write well … and the ability to influence others' behaviour around cyber security" (p. 89). The report interchangeably uses the terms soft and complementary skills, but we will use the latter when referring to their work. The report (DCMS, 2022) showed the extent to which cybersecurity organizations were aware of the importance of transferable skills. For example, when organizations were asked to rate how important it is for those in cybersecurity roles to have complementary skills, using a scale of 0 (*not at all*) to 10 (*essential*), organizations indicated an average score of 8.4 out of 10, and 37% indicated 10. As well as identifying this importance, they noted that scores have increased by 10% since the same survey was conducted in 2021. According to this survey (DCMS, 2022), 26% of organizations stated that over the last 12 months, job applicants for cybersecurity roles had been lacking in communication, leadership, management, or sales and marketing skills and that because of this it had stopped the organization meeting their business goals to some or a great extent. These figures are higher than the 2021 survey (when it was 18%), possibly indicating a worsening situation.

In addition to the quantitative survey data, the DCMS Cyber Security Survey researchers also interviewed cybersecurity leaders and asked them to reflect on the need for "complementary" skills in the cybersecurity sector (using their previous definitions). An analysis of this data revealed that three types of skills were mentioned most frequently: (i) being able to communicate effectively with a range of people, such as senior managers and service providers; (ii) the ability to write well was mentioned in terms of technical report writing as well as in writing bids for new client contracts; and (iii) the importance of being able to persuade noncybersecurity staff to follow cyber security policies, such as the skill to influence behavior. We suggest that psychology graduates may possess many of these skills needed in the cybersecurity industry, for example, one of the PLs proposed by McGovern et al. (2010) addresses these communication skills, "communicating effectively in different modes and with many different audiences." The DCMS report also discusses the demographic background of those working in cybersecurity and although this is outside the scope of this article, the authors propose that the cybersecurity industry needs to be more representative of the population, such as increasing the number of women and people from diverse ethnic backgrounds in the workforce. The DCMS Cyber Security Survey researchers then state that without this diversity of skills and talent, the industry is left with what has been termed a "cybersecurity skills gap."

Aims of the Study

The aims are to:

(i) explore psychology students' understanding of what cybersecurity work involves and their views of the knowledge and skills needed to work in cybersecurity;
(ii) identify how psychology students perceive PLs as being relevant to working in psychology and cybersecurity, and
(iii) a subsidiary aim was to inform the development of further questions for a more extensive survey and open-ended questions for individual interviews.

Method

Participants

A total of 66 students participated in an online survey; 12 were male, 54 were female and no students responded to the options "other" or "prefer not to say." Participants ranged from 19 to 36 years of age, but the majority (n = 61) were aged between 19 and 23 years with a mode of 20 years. The participants came from 3-year groups studying for a BSc (Hons) Psychology degree at one university [*deleted for anonymous review*]. There were 19 first-year students, 40 second-year students, and seven students who had just completed the final year of the degree.

Materials

A short online survey contained two open-ended and two closed questions. Participants were asked: "What do you think people who work in the cybersecurity industry do? Please add some activities you think they may undertake," and "Can you think of any specific skills gained in your psychology degree that would be useful in the cybersecurity industry?" Students were then asked to judge the importance of nine PL items to careers in cybersecurity and psychology. The items came from those identified by McGovern et al. (2010) and were slightly adapted (item 4 was adapted to apply specifically to the work environment). Participants were presented with the same items regarding the two disciplines of interest in this study. Specifically, they were asked how important they thought each of these PL items was for a cybersecurity and psychology career; a specific career or role in each field was not defined. Responses to these nine items were collected using a scale from 1 (*not important*) to 7 (*very important*); the items are listed below:

1. Having a basic knowledge of psychology.
2. Using scientific thinking and the disciplined analysis of information to evaluate alternative courses of action.
3. Taking a creative and skeptical approach to problem solving.
4. Applying psychological principles to personal, social, and organizational issues in the *work environment.*
5. Acting ethically.
6. Being competent in using and evaluating information and technology.
7. Communicating effectively in different modes and with different audiences.
8. Recognizing, understanding, and fostering respect for diversity.
9. Being insightful and reflective about your own and others' behavior and mental processes.

Procedure

Ethical approval was granted prior to advertising and recruitment to the study. Approval for the study was granted by the University Research Ethics Committee (Ethics Code: 39255) and was conducted in accordance with The British Psychology Society Code of Ethics. An advert inviting students to participate in the study was added to the SONA student research participation site. If students clicked the link, they were taken to the Qualtrics online survey site where they were provided with an information sheet. After reading this information, students were asked to either agree or disagree to provide their informed consent to participate. If they provided consent the survey opened and students could answer questions or leave them blank, but they were not allowed to go back through their answers to avoid changing qualitative responses once the PL items were viewed. The online survey link was available on the SONA site for one month towards the end of the academic year. Participants received experimentation credits in return for participation and after completion, they were sent a debrief form.

Results

Analysis of Qualitative Data

The responses to the two open-ended questions were analyzed using content analysis. This was considered the most appropriate analytical method as responses were brief and lacked the detail needed for qualitative inferences to be made through analyzing the meaning of the words and concepts, such as by using thematic analysis (Braun & Clarke, 2006). The key feature of all forms of content analysis is that the keywords of text are classified into much smaller content categories. Stemler (2001) states that content analysis "allows inferences to be made which can then be corroborated using other methods of data collection" (p. 1) and therefore it is appropriate for this study which aims to analyze and combine qualitative and quantitative data. Vears and Gillam (2022) recommend inductive content analysis (ICA), also known as qualitative content analysis, for relatively small-scale and non-complex research. This study meets these criteria. The process involves initial coding where codes are assigned to over-arching content categories. For example, for question 1 the comments were divided into those relating to technical issues and those relating to human issues. This is then followed by comparing, grouping, and sub-dividing groups of codes, which results in final content categories and sub-categories rather than "themes." A "content category" is a broad idea or concept within which a number of more specific content codes have been grouped. One of the researchers completed the content analysis and no interrater reliability was carried out for this small-scale exploratory study. The first question aimed to gather views from psychology students as to their understanding of what people working in the cybersecurity industry do. The second question asked students what skills gained in a psychology degree would be useful to work in the cybersecurity industry.

As shown in Table 1, two categories emerged from the responses to: "What do you think people who work in the cybersecurity industry do? Please add some activities you think they may undertake." Most comments (n = 39) related to Category 1 "technical activities" and there were seven smaller sub-categories reflecting specific tasks. Category 2 "human behaviour" contained comments which specifically mentioned people and was divided into two sub-categories: (a) protect victims and training (n = 7), and (b) identify and prevent attackers (n = 13). Table 1 provides example quotes to give a flavor of the types of responses in each category and the full data can be found in Supplemental Table 4.

Participants were asked, "Can you think of any specific skills gained in your psychology degree that would be useful to work in the cybersecurity industry?" The analysis revealed three categories which can be seen in Table 2: Category 1 "technical skills" (n = 8) was divided into two sub-categories, "using programmes/software" and "technology/computer/maths skills." Category 2 "transferable skills" contained the largest number of comments (n = 25) and was further divided into six sub-categories, representing different types of transferable skills. The third category, "psychology content" (n = 12) was divided into six sub-categories representing different areas of psychology deemed useful in cybersecurity to predict and/or prevent cybercrime. Table 2 provides example comments to give a flavor of the types of responses in each category and the full data are in Supplemental Table 5.

Analysis of Quantitative Data

To explore the extent to which students recognized the importance of the skills and knowledge they learned in their psychology degree, they were asked to consider the extent to which each of the nine PL items identified by McGovern et al. (2010) was important for a psychology career and a

Table 1. Analysis of Responses to the Question, "What Do You think people Who work in the cybersecurity industry Do? Please add some activities You think they May undertake."

Category	Sub-category	Example comments
1. Technical activities		
	(a) General protection of computers, networks, and systems (n = 14)	• Keeps websites safer • Information technology security • Protect computer networks and systems
	(b) Specific protection of data, software, and finance from theft/compromise (n = 5)	• Protecting data online from being taken or compromised • Protect software, protect accounts, and networks from viruses
	(c) Firewalls (n = 3)	• Look for weak spots in an online security firewall
	(d) Threat analysis (n = 3)	• Analyze perceived threats online
	(e) Monitor systems (n = 3)	• Take steps to monitor and protect computer networks and systems
	(f) Reduce or prevent (n = 5)	• Reduce the risk of cyber attack • Prevent online fraud such as scams. and cyber crimes
	(g) Miscellaneous (n = 6)	• Advising companies on cybersecurity • Health and safety checks
2. Human behavior		
	(a) Protect victims/training (n = 7)	• Scam protection (from people sending phishing emails and cold calls) • Training people how to avoid being scammed/hacked
	(b) Identify and prevent attackers (n = 13)	• Profile cyber criminals • Blocking/preventing cyberbullies (mentioned twice) • Countering the behavior of cybercriminals as well as being able to anticipate and predict their behaviors and crimes

cybersecurity career. A comparison of students' views of skills needed to work in psychology and cybersecurity can be seen in Table 3, which shows the results of *t*-tests highlighting that responses to eight out of nine items were significantly different. Seven out of these eight items were judged to be higher for psychology careers than cybersecurity careers. Item 6, "being competent in evaluating information and technology," was judged to be higher for cybersecurity than for psychology careers. There were no significant differences for item 3 "having a creative and sceptical approach to problem-solving." Table 3 presents the PLs in the order from the highest rated to the lowest rated for cybersecurity. It can be seen that the two lowest-rated PLs are those specifically mentioning psychology. The two highest items relate to information technology and ethics.

Discussion

Summary of Results

Two categories emerged from the analysis of responses to the question, "What do you think people who work in the cybersecurity industry do?" As expected, most of the comments related to

Table 2. Analysis of Responses to the Question, "Can You think of any specific skills gained on your psychology degree that would Be useful to work in the cybersecurity industry?"

Category	Sub-category	Example comments
1. Technical activities		
	(a) Using programs/software (n = 5)	• I have learned how to use different types of programs, such as JASP and SPSS • Different types of Excel and computer-based analysis tasks
	(b) Technology/computer/maths skills (n = 3)	• Computer skills
2. "Transferable" skills		
	(a) Critical thinking/critical analysis (n = 9)	• Critically analyzing data • Critical thinking and analyzing certain events • Analyzing and problem-solving/thinking critically
	(b) Analyzing/evaluating data (n = 5)	• The ability to process and evaluate quantitative and qualitative data • In-depth evaluation
	(c) Attention to detail (n = 4)	• Keeping an eye on detail
	(d) Communication skills (n = 3)	• Communicate in a more professional manner • Communication skills
	(e) Problem solving/creative thinking (n = 3)	• Creative thinking for problem solving
	(f) Ethical training (n = 2)	• Ethical training
3. Psychology content		
	(a) Understanding of forensic psychology (n = 3)	• Using knowledge of forensic psychology to try and anticipate the behaviors and motives behind cybercrime • Understanding of why people may hack, which allows for me to anticipate future breaches and be able to prevent them.
	(b) Understanding of cognition (n = 2)	• Perception memory
	(c) Ability to analyze behavior (n = 3)	• Being able to analyze and recognize people's behavior
	(d) Understanding of individual differences (n = 2)	• Understanding people's differences (culture, ethnicity, social status, sexuality, etc.),
	(e) Understanding of emotion (n = 1)	• Understanding of emotion and people's reaction to it
	(f) Understanding of mental health conditions (n = 1)	• Awareness of mental health conditions, their symptoms, and how they may affect a person's state of mind, thinking process, actions, and communication levels

technical activities, however, the comments relating to human behavior demonstrated that students recognized the complex role of people in cybersecurity. Moreover, they identified mechanisms relating to both protecting the victims and preventing attackers. When asked, "Can you think of

Table 3. Results of T-tests Comparing the Importance of Nine Psychological Literacy Items for Careers in Psychology and Cybersecurity, Measured Using a Scale of 1 (*Not Important*) to 7 (*Very Important*).

	Cybersecurity		Psychology			
Psychological Literacy Item	*M*	(*SD*)	*M*	(*SD*)	*t*(64)	*p*
6. Being competent in evaluating information and technology	6.523	(0.691)	5.554	(2.032)	5.570	.000**
5. Acting ethically	6.292	(1.710)	6.785	(0.328)	3.140	.003**
2. Scientific thinking and analysis to evaluate alternatives	6.030	(1.187)	6.461	(0.721)	3.554	.000**
8. Recognizing and fostering respect for diversity	6.015	(1.797)	6.723	(0.547)	4.532	.000**
9. Being insightful and reflective about own and others' behavior	5.892	(1.816)	6.846	(0.163)	5.691	.000**
3. Having a creative and skeptical approach to problem solving	5.800	(1.694)	5.862	(2.027)	0.360	.720
7. Communicating effectively in different modes and with many different audiences	5.692	(2.199)	6.246	(1.102)	4.140	.000**
4. Applying psychological principles	5.456	(1.782)	6.527	(1.003)	5.070	.000**
1. Basic knowledge of psychology	4.954	(2.670)	6.656	(0.826)	7.263	.000**

**Significant at 1%.

any specific skills gained on your psychology degree that would be useful to work in the cybersecurity industry?" again as expected, many of the comments related to "technical skills." However, most of the comments were categorized as transferable skills, which covered many of the PLs suggested by McGovern et al. (2010). A third category reflecting psychology content showed that students identified knowledge from different areas in psychology that were useful in cybersecurity to predict and/or prevent cybercrime.

Not surprisingly, the analysis of quantitative data found that for seven of the nine items, students perceived the PLs as more important for working in psychology, than in cybersecurity. The item, "being competent in evaluating information and technology," was judged to be more important for working in cybersecurity and there was no significant difference for the item "having a creative and sceptical approach to problem solving." Despite the significant differences, it is noteworthy that students still rated highly the importance of transferable skills for working in cybersecurity (indicated by the means for all items being above the mid-point of 3.5).

The Importance of PL for Working in the Field of Cybersecurity

There is a growing recognition of how aspects of PL relate to working in "non-psychology" careers (Machin & Gasson, 2022). Our study is the first to link PL to working in cybersecurity, which is one of several fast-growing occupations. Below we identify how together the qualitative and quantitative data can inform our understanding of the way that each PL is important for people working in cybersecurity. We finish this section by suggesting some ways that instructors can make students aware of the value of their PLs to working in cybersecurity.

PL item 1, "Basic knowledge of psychology." The qualitative and quantitative data showed a different pattern for this literacy. In the qualitative data, participants commented on the usefulness of knowledge of different areas in psychology (such as forensic psychology, cognition, individual differences, and emotion), which were identified in the literature review as being important (Andrade & Yoo, 2019; Rajagulasingam & Taylor, 2022; Whitty, 2019). However, the quantitative data showed that this PL was the lowest rated. This indicates that although this PL is identified as useful for cybersecurity (as it is above the mid-point score of 3.5), students see it as more important for a psychology career. The implication of this finding is that to encourage more psychology graduates to consider a role in cybersecurity, awareness-raising initiatives may be needed to highlight what the cybersecurity industry requires and to show psychology students where there is a match with the knowledge they have learned during their degree.

PL item 2, "Scientific thinking and analysis to evaluate alternatives." It is important that those working in cybersecurity are able to apply a scientific approach to evaluate cybersecurity incidents (Bauer, Truxillo, Jones, & Brady, 2020). The quantitative data revealed that this item was judged to be significantly more important for a psychology career than a cybersecurity career. The qualitative data identified five comments under the sub-category "analysing and/or evaluating data" showing that psychology students clearly recognized the wide range of quantitative and qualitative methods they could apply to collect and analyze data to evaluate cybersecurity incidences and to design and evaluate interventions. In summary, both sets of data showed some recognition of the importance of scientific thinking in both careers.

PL item 3, "Having a creative and sceptical approach to problem solving." The results showed that the means for this literacy were similar for psychology and cybersecurity careers and not significantly different, so perhaps this literacy was judged as equally important to both careers. The analysis of the qualitative data only showed three comments related to this PL, categorized under the sub-category "creative thinking or problem-solving" as being important in cybersecurity. The lack of comments and nonsignificance of the data may relate to students not being fully aware of this literacy. Student recognition of problem-solving skills often only occurs in the latter part of a degree course (e.g., see the learning outcomes for levels 4 (certificate), 6 (diploma), and 7 (bachelor degree) as defined by the Framework for Higher Education Qualifications in the United Kingdom (FHEQ, 2014). The sample in this study was predominantly in the first or second year of their U.K. degree course (levels 4 and 5), with very few in the third year (level 6).

PL item 4 "Applying psychological principles." The qualitative and quantitative data showed a different pattern for this literacy. The key psychological skill identified in the qualitative data was related to critical thinking, which was noted by nine participants. However, the quantitative data showed that the second lowest-rated PL was related to psychology skills, the aspects emphasized by researchers and cyber practitioners (Department for Digital, Culture, Media & Sport, 2022) as important. This indicates that although this PL is identified as useful for cybersecurity, students do not see it as important. The implication of this finding is that to encourage more psychology graduates to consider a role in cybersecurity, awareness-raising initiatives may be needed to highlight what the cybersecurity industry requires and to show psychology students where there is a match with the skills they have learned during their degree.

PL item 5, "Acting ethically." This item was judged to be significantly more important for a psychology career than a cybersecurity career. However, it was surprising that only two participants identified acting ethically as important in cybersecurity. Many aspects of the psychology code of ethics developed by international psychology associations are relevant to understanding illegal online activities. For example, one of the key principles in the BPS Code of Ethics (Oates et al., 2021) is respect for the dignity of people and when applying this to cybersecurity it would mean understanding issues relating to privacy and confidentiality, for example, public and private privacy settings and requiring consent among other things. In the later section, we suggest ways to raise awareness of the applicability of ethics training to careers outside of psychology could take place.

PL item 6, "Being competent in evaluating information and technology." The quantitative data showed that this literacy was judged to be significantly more important to working in a cybersecurity career compared to a psychology career. The qualitative data also revealed that psychology students recognized the usefulness of interacting with a variety of software (such as statistics software, experiment generators, and referencing tools) for a cybersecurity career. Eight students gave examples of the technical skills developed during the psychology degree as important in cybersecurity. This is a relatively small proportion of the total number of participants and therefore might suggest a need to boost confidence in and awareness of the application of technical competencies developed within psychology courses to careers outside of psychology.

PL item 7, "Communicating effectively in different modes and with many different audiences." This item was judged to be significantly more important for a psychology career than a cybersecurity career. Psychology students can be exposed to different audiences when they collect data in the community or if they undertake placements (e.g., in mental health environments). However, many students are not exposed to diverse audiences, so it was not surprising that only two students recognized this literacy as important in the qualitative data. Quality assurance and professional bodies such as the QAA and BPS in the United Kingdom (QAA, 2023) encourage psychology providers to enable activities to enable students to work in real-world contexts and to consider using samples that do not come from the undergraduate psychology population. These experiences have been shown to develop many PLs, however, it has been reported that such activities can be time-consuming for academics to set up and can be fraught with ethical issues (Taylor, 2019).

PL item 8, "Recognising, understanding, and fostering respect for diversity." This item was judged to be significantly more important for a psychology career than a cybersecurity career. However, only two students recognized the usefulness of understanding individual differences in cybersecurity. It is important that those working in cybersecurity are aware of the individual differences in susceptibility to scams and differences in the likelihood of adhering to secure practices (Williams et al., 2017).

PL item 9, "Being insightful/reflective about your own/others' behaviour and mental processes." This item was judged to be significantly more important for a psychology career than a cybersecurity career, which would be expected; additionally, students rated this literacy as the most important out of the nine literacies for a career in psychology. However, surprisingly this literacy was identified only once in the qualitative analysis, where one student indicated "understanding of mental health conditions" as a useful skill for a career in cybersecurity and it could be that the key attraction for students who choose to study psychology is to develop this skill; this is in line with some the findings of Heritage et al. (2016). The implication of this is that the perceived lesser importance of this literacy for cybersecurity may be a disincentive to work in cybersecurity, but further research is needed to explore this.

Methods for Enhancing Awareness of PLs for Working in the Field of Cybersecurity. One way to enhance awareness would be through modules that cover career advice where PLs that could be applied in a cybersecurity career could be highlighted. For example, students could be asked to generate a list of concepts and skills developed during their course that are relevant to cybersecurity, or even as a starting point the categories reported in Tables 1 and 2 could be used as a focus for a group discussion. Students could be asked to search for and summarize research articles that identify the knowledge and skills needed to succeed in cybersecurity; this activity could take place in small teams where several of the fastest-growing occupations (including cybersecurity) could be covered. The team product could be an infographic, presentation, or pitch explaining why psychology is a good fit for their assigned occupation. In modules dealing with ethics, new initiatives could be implemented to raise awareness of the applicability of ethics training to cybersecurity, for example, students could be asked to discuss how the concept of ethics applies to privacy in online environments.

Challenges and Opportunities

Despite some recognition of the skills gap in cybersecurity provision, there needs to be more research undertaken within the disciplines of human resources management and organizational psychology, a recommendation emphasized recently by Bauer et al. (2020) and Dalal et al. (2022). Most of the published research relating to the cybersecurity skills gap comes from the disciplines of computer science, information systems, information technology, and the law (Dreibelbis et al., 2018) and focuses on the technical skills gap, rather than research on the social sciences to identify or address the transferable skills gap.

There are many opportunities for psychology graduates to work in cybersecurity, and governments around the world have identified this as an area of current and future job growth (Ikeda, Marshall, & Zaharchuk, 2019). More work needs to be done regarding making recruiters and careers services aware of the role of psychology and human factors in cybersecurity. A key challenge is to provide appropriate training. Globally, Higher Education Institutions provide several undergraduate and postgraduate courses and modules teaching cybersecurity, however, these tend to be located in computer science or computing departments and often contain little psychological content and are taught by nonpsychologists. There are some opportunities for psychology graduates to be employed directly in cybersecurity organizations through employers recruiting graduates with a non-specific degree. Once a graduate is employed within the cybersecurity industry, to become a practicing cybersecurity specialist further education would be required, as discussed in the report on cybersecurity skills published by the Department for Digital, Culture, Media and Sport (2022). This can take the form of industry-run certification schemes, or it could involve studying at a Higher Education Institution for a postgraduate qualification, either while working part-time or full-time. At the time of writing, the U.K. government has introduced a scheme called “Upskill in Cyber” (2023) which is intended to bridge what they refer to as the “digital skills gap” in the United Kingdom.

There is a need to enhance psychology students’ awareness of their skills in nonpsychology roles in computing and cybersecurity and suggested ways to do this have been covered in the previous section. While technical and cyber security modules are starting to be taught within psychology degrees, they are still relatively rare and are often limited to one or two lectures relating to cybercrime within Forensic Psychology modules. We also suggest that collaborations between educators working in psychology and cybersecurity would be fruitful, to enhance awareness of work opportunities in the cybersecurity industry for psychology students.

Methodological Limitations and Future Research

It is interesting to note that many of the literacies that students rated highly for working in cybersecurity weren’t necessarily the aspects they noted in their open-ended comments. This might be explained by the different wording used to ask the open-ended questions, focusing on the “usefulness,” while the wording of the instructions was to consider the “importance” of the PLs for working in the two careers. It is important to be consistent in the question wording used and this will be addressed in future data collection. In addition, a specific career or role in each field was not defined. As this was not defined, there was no way of knowing whether participants were thinking about the same career options in psychology or the same roles in the field of cybersecurity when responding to the survey. This will be addressed in future data collection by providing a brief overview of each field and potentially to ask students to select a specific role. When students were asked to judge the importance of the PL items to careers in cybersecurity and psychology, the order was always the same. On reflection, there could have been an order effect so the presentation of each career should have been randomized.

The results from this study will inform questions to be included in three follow-up studies, fulfilling the third aim of this evaluation. The first study will involve the distribution of an online survey to a large international sample of psychology and cybersecurity students to identify if the findings from this study are replicated with a larger and more diverse sample. Also, this study will explore gender and age differences. A second study will involve individual interviews with students to explore perceived barriers and opportunities and these will be analyzed in depth using thematic analysis (Braun & Clarke, 2006). The findings showed that while students had a good understanding of the diverse skills and knowledge involved in cybersecurity, the number of comments relating to the nine PL items was relatively small, and therefore, awareness-raising initiatives will take place within one university. The form of these initiatives has not yet been finalized but may include some of the suggestions we made earlier with the aim of enhancing students' understanding of how their psychology literacies are relevant to various roles in the cybersecurity industry. An evaluation (study 3) will assess whether these initiatives affect student's perceptions, compared to a comparison group at another university where initiatives are not undertaken. Following the publication of our findings, we would invite instructors to use our suggestions to enhance students' awareness of their PL for cybersecurity and for them to assess the effectiveness of any teaching interventions they design.

Conclusion

This report supports the views of many psychologists to share the benefits that psychological science has identified to enhance society, sometimes referred to as "giving Psychology away" (Banyard & Hulme, 2015). By employing psychology graduates in the cybersecurity industry, psychological knowledge, and expertise are being shared outside of psychology to enhance the effectiveness of roles within the cybersecurity industry and this could eventually have a positive influence on society through reduced cybersecurity incidents.

Acknowledgments

We would like to thank the anonymous reviewers for their thorough and constructive reviews of this article, which led to significant improvements.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Jacqui Taylor https://orcid.org/0000-0002-2145-5077

Supplemental Material

Supplemental material for this article is available online.

References

Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications*, *48*, 102352. https://doi.org/10.1016/j.jisa.2019.06.008

Banyard, P., & Hulme, J. A. (2015). Giving psychology away: How George Miller's vision is being realised by psychological literacy. *Psychology Teaching Review*, *21*(2), 93–101. https://doi.org/10.53841/bpsptr.2015.21.2.93

Bauer, T. N., Truxillo, D. M., Jones, M. P., & Brady, G. (2020). Privacy and cybersecurity challenges, opportunities, and recommendations: Personnel selection in an era of online application systems and big data. In S. E. Woo, R. Proctor, & L. Tay (Eds.), *Big data in psychological research* (pp. 393–409). APA. https://doi.org/10.1037/0000193-018

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261–283. https://doi.org/10.1080/1068316X.2013.772180

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

Cranney, J., Dunn, D. S., Hulme, J. A., Nolan, S. A., Morris, S., & Norris, K. (2022, May). Psychological literacy and undergraduate psychology education: An international provocation. *Frontiers in Education*, *7*. https://doi.org/10.3389/feduc.2022.790600

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2022). Organizational science and cybersecurity: Abundant opportunities for research at the interface. *Journal of Business and Psychology*, *37*(1), 1–29. https://link.springer.com/article/10.1007/s10869-021-09732-9

Department for Digital, Culture, Media and Sport. (2022). *Cyber security skills in the UK labour market 2022*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf

Dreibelbis, R. C., Martin, J., Coovert, M. D., & Dorsey, D. W. (2018). The looming cybersecurity crisis and what it means for the practice of industrial and organizational psychology. *Industrial and Organizational Psychology*, *11*(2), 346–365. https://doi.org/10.1017/iop.2018.3

Esentire. (2023). *Official cybersecurity jobs report*. https://www.esentire.com/resources/library/2023-official-cybersecurity-jobs-report

FHEQ. (2014). *The frameworks for higher education qualifications of UK degree-awarding bodies*. QAA. Accessed October 16, 2023, from https://www.qaa.ac.uk/docs/qaa/quality-code/qualifications-frameworks.pdf?sfvrsn=170af781_18

Goh, P. (2021). Humans as the weakest link in maintaining cybersecurity: Building cyber resilience in humans. In M. Khader, W. X. T. Chai, & L. S. Neo (Eds.), *Introduction to cyber forensic psychology: Understanding the mind of the cyber deviant perpetrators* (pp. 287–305). World Scientific. https://doi.org/10.1142/12164

Heritage, B., Roberts, L. D., & Gasson, N. (2016). Psychological literacy weakly differentiates students by discipline and year of enrolment. *Frontiers in Psychology*, *7*, 162. https://doi.org/10.3389/fpsyg.2016.00162

Ikeda, K., Marshall, A., & Zaharchuk, D. (2019). Agility, skills and cybersecurity: Critical drivers of competitiveness in times of economic uncertainty. *Strategy & Leadership*, *47*(3), 40–48. https://doi.org/10.1108/SL-02-2019-0032

Machin, T., & Gasson, N. (2022). An introduction to careers in psychological science. In T. Machin, T. Machin, C. Jeffries, & N. Hoare (Eds.), *The Australian handbook for careers in psychological* *science* (pp. 1–22). University of Southern Queensland. https://usq.pressbooks.pub/psychologycareers/chapter/what-is-psychological-science/

Machin, T., Machin, T., Jeffries, C., & Hoare, N. (2022). *The Australian handbook for careers in psychological science*. University of Southern Queensland. https://usq.pressbooks.pub/psychologycareers/chapter/what-is-psychological-science/

McAlaney, J., Thackray, H., & Taylor, J. (2016). The social psychology of cybersecurity. *The Psychologist*, *29*, 686–689. http://eprints.bournemouth.ac.uk/22052/1/mctf15.pdf

McGovern, T., Corey, L., Cranney, J., Dixon, W., Holmes, J. D., Kuebli, J. E., Ritchey, K. A., Smith, R. A., & Walker, S. J. (2010). Psychologically literate citizens. In D. F. Halpern (Ed.), *Undergraduate education in psychology: A blueprint for the future of the discipline* (pp. 9–27). American Psychological Association. https://doi.org/10.1037/12063-001.

Murdoch, D. D. (2016). Psychological literacy: Proceed with caution, construction ahead. *Psychology Research and Behavior Management*, *9*, 189–199. https://doi.org/10.2147/PRBM.S88646

Oates, J., Carpenter, D., Fisher, M., Goodson, S., Hannah, B., Kwiatowski, R., Prutton, K., Reeves, D., & Wainwright, T. (2021). *BPS code of human research ethics*. Leicester: British Psychological Society. https://doi.org/10.53841/bpsrep.2021.inf94

Proudfoot, J. G., Wilson, D., Valacich, J. S., & Byrd, M. D. (2018). Saving face on Facebook: Privacy concerns, social benefits, and impression management. *Behaviour & Information Technology*, *37*(1), 16–37. https://doi.org/10.1080/0144929X.2017.1389988

QAA. (2023). *Quality assurance agency subject benchmark statement for psychology*. https://www.qaa.ac.uk/docs/qaa/subject-benchmark-statements/subject-benchmark-statement-psychology.pdf

Rajagulasingam, C., & Taylor, J. (2022). The roles of self-control, need for cognition, impulsivity and viewing time in deception detection using a realistic e-mail phishing task. 2021 APWG 16th Annual Symposium on Electronic Crime Research (eCrime), December 2021, pp. 1–5. https://doi.org/10.1109/eCrime54498.2021.9738794

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, *9*(4), 475–480. https://doi.org/10.1037/ppm0000247

Spencer, S. M. (2021). A comprehensive, iterative, and integrated model for developing psychology workforce literacy. *Canadian Psychology*, *62*(4), 409–419. https://doi.org/10.1037/cap0000309

Stemler, S. (2001). An overview of content analysis. *Practical Assessment, Research, and Evaluation*, *7*, Article 17. https://doi.org/10.7275/z6fm-2e34

Taylor, J. (2019). Psychological literacy for all: An overview of this 'literacy' and how it is relevant for students of all disciplines. EDULEARN19, the 11th Annual International Conference on Education and New Learning Technologies, Palma de Mallorca, Spain, July 1–3, 2019, pp. 4497–4501. IATED Digital Library. ISBN: 978-84-09-12031-4. https://doi.org/10.21125/edulearn.2019.1126

Taylor, J., McAlaney, J., Foster, J. L., Bello, A., Maurushat, A., Dale, J. (2020). Incorporating psychology into cyber security education: A pedagogical approach. In M. Bernhard, et al. (Eds.), *Financial cryptography and data security* (Vol. 12063, pp. 207–217). FC 2020. Lecture Notes in Computer Science. Springer. https://doi.org/10.1007/978-3-030-54455-3_15

Thackray, H., Richardson, C., Dogan, H., Taylor, J., & McAlaney, J. (2017). Surveying the hackers: The challenges of data collection from a secluded community. Proceedings of 16th European Conference on Cyber Warfare and Security, pp. 745–748. https://www.cs.ucd.ie/2017-eccws-ucd/

Upskill in Cyber UK. (2023). *Upskill in cyber UK programme application page*. https://www.sans.org/mlp/upskillcyber-uk/

Vears, D. F., & Gillam, L. (2022). Inductive content analysis: A guide for beginning qualitative researchers. *Focus on Health Professional Education: A Multi-Disciplinary Journal*, *23*(1), 111–127. https://doi.org/10.11157/fohpe.v23i1.544

Whitty, M. T. (2018). It's just a game: Developing a framework to understand cyberfraud from a Nigerian cultural perspective. *International Journal of Cyber Criminology*, *12*(1), 97–114. https://doi.org/10.5281/zenodo.1467848

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095

Whitty, M. T. (2021). Developing a conceptual model for insider threat. *Journal of Management & Organization*, *27*(5), 911–929. https://doi.org/10.1017/jmo.2018.57

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412–421. https://doi.org/10.1016/j.chb.2017.03.002

Author Biographies

Jacqui Taylor works at Bournemouth University as an associate professor where she has held a number of roles to enhance student's employability involving enhancing awareness of psychological literacy and developing technological skills. Jacqui has led units in Social Media, Social Psychology, and Cybersecurity and she developed a BSc(Hons) degree in Cyberpsychology. Jacqui is a senior fellow of the UK Higher Education Academy and has held educational leadership roles nationally as Chair of the BPS Division of Academics, Researchers, and Teachers in Psychology, and internationally as President of the International Council of Psychology Educators. Jacqui is a Chartered Psychologist and Associate Fellow of the British Psychological Society (BPS) and has served on many BPS committees. Jacqui's research investigates a wide variety of impacts of the Internet on human interaction and she has published research on morality and video games, the development of online identity, social media and self-esteem, and the relationship between online trust and online deception. She has published in and regularly reviews for journals related to cyberpsychology, human–computer interaction, computing, and psychology.

Professor Monica Whitty is the head of the Department of Software Systems and Cybersecurity and is a professor of Human Factors in Cyber Security. She has been a member of the World Economic Forum Cyber Security Centre and was a member of the WEF Cyber Security Global Futures Committee. Prof Whitty's academic career began in Australia working at Macquarie University and the University of Western Sydney, before moving to the UK (2003) and then returning home to Australia (2018). In the UK, she worked for universities in the Russell Group (Queen's University, Belfast; University of Warwick), and The 1994 Group Universities (University of Leicester). In Australia, she previously worked at the University of Melbourne before commencing her post at UNSW in 2020. She was the founder and the Director of the UNSW Institute for Cyber Security (IFCYBER). Professor Whitty has worked in a GCHQ-accredited Cyber Security Centre in the UK at the University of Warwick and has held an honorary post at the University of Oxford at the Oxford Martin School and the Oxford Internet Institute, and an honorary Professorship at the Institute of Royal Holloway, University of London. Monica has extensive experience in leading large interdisciplinary, international teams on funded projects. Professor Whitty has been awarded significant research funding (> $15 million AUD) and has led most of her projects. She has extensive experience in teaching at all levels and in the development of successful Masters courses. Prof Whitty is the author of over 100 articles and five books. She is a leading expert on cyber fraud (esp. romance scams), identities created in cyberspace, online security risks, behavior in cyberspace, insider threats, as well as detecting and preventing deception, such as cyber scams and mis/disinformation. Monica is also currently on a talkback radio program on ABC Cairns to provide help and feedback to prevent scam victimization.