Modelling the ethical priorities influencing decision-making in cybersecurity contexts

Bakhtiar Sadeghi and Deborah Richards
School of Computing, Macquarie University, Sydney, Australia
Paul Formosa
Department of Philosophy, Macquarie University, Sydney, Australia, and
Mitchell McEwan, Muhammad Hassan Ali Bajwa, Michael Hitchens and Malcolm Ryan
School of Computing, Macquarie University, Sydney, Australia

Received 1 September 2022
Revised 5 December 2022
Accepted 3 April 2023

Abstract

Purpose – Cybersecurity vulnerabilities are often due to human users acting according to their own ethical priorities. With the goal of providing tailored training to cybersecurity professionals, the authors conducted a study to uncover profiles of human factors that influence which ethical principles are valued highest following exposure to ethical dilemmas presented in a cybersecurity game.

Design/methodology/approach – The authors' game first sensitises players (cybersecurity trainees) to five cybersecurity ethical principles (beneficence, non-maleficence, justice, autonomy and explicability) and then allows the player to explore their application in multiple cybersecurity scenarios. After playing the game, players rank the five ethical principles in terms of importance. A total of 250 first-year cybersecurity students played the game. To develop profiles, the authors collected players' demographics, knowledge about ethics, personality, moral stance and values.

Findings – The authors built models to predict the importance of each of the five ethical principles. The analyses show that, generally, the main driver influencing the priority given to specific ethical principles is cultural background, followed by the personality traits of extraversion and conscientiousness. The importance of the ingroup was also a prominent factor.

Originality/value – Cybersecurity professionals need to understand the impact of users' ethical choices. To provide ethics training, the profiles uncovered will be used to build artificially intelligent (AI) non-player characters (NPCs) to expose the player to multiple viewpoints. The NPCs will adapt their training according to the predicted players' viewpoint.

Keywords Ethical training, Cybersecurity ethics, Ethical fading, Ethical principles, Serious games

Paper type Research paper

1. Introduction

Emerging technologies such as cloud computing facilitate access and expand usage of software products for end users. These emerging technologies generate huge volumes of data, including sensitive (e.g. personal and financial) data, that need to be protected against threats and made available for appropriate access using increasingly complex cybersecurity

This work is funded by an Australian Research Council Discovery Grant: DP200102131 - Cybersecurity ethics training simulations for values-based decision-making.

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 3 No. 2, 2023
pp. 127-149
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-09-2022-0015

techniques. Accordingly, there is a large body of research, supporting technology and policies to address cybersecurity threats to protect the confidentiality, integrity and availability (CIA) of data and services (Brey, 2007). However, the human factors within a cybersecurity system related to ethical decision-making, ranging from behaviours of system administrators and software developers to cybersecurity domain experts, are a vulnerability gap that has received comparatively less attention.

We need to trust our techniques, such as machine learning algorithms, and policies being developed by cybersecurity experts to protect our data against cyber threats. To protect data, we rely on the domain experts who design and implement these techniques, algorithms and policies. Individual domain experts who develop and implement cybersecurity systems, as well as those who make decisions at higher levels of organisational hierarchies, need to understand the human aspects (such as social engineering (Mann, 2008)) of the solutions they design. Solutions will fail to achieve their intended goals if the domain experts who design them are not cognisant of these human aspects which is a key system vulnerability (Safa *et al.*, 2016; Nobles, 2018). To deal with socio-technical issues within an organisation, employees (e.g. designers and managers) may receive training via various mediums, such as online courses, live role-playing games or computer-based serious video games [1]. However, all of these approaches have limitations in transferring knowledge and skills to real situations that will be impacted by human factors, roles and skills (Gee, 2007). Of particular relevance in the context of ethical dilemmas is the situation where a human's personal values override organisational norms, and this results in a decision to breach organisational policies (Schwartz, 2012; Christen *et al.*, 2017). For instance, individuals who value their ingroup highly and seek to follow its social norms and practices might fail to change their password regularly in accordance with an organisational policy because they prioritise acting in accordance with the implicit norms of their ingroup (assuming there is no automated password expiring policy in place).

To study cybersecurity ethical decision-making, we used as our framework the principlist approach developed by Formosa *et al.* (2021). This framework includes five ethical principles, namely beneficence (cybersecurity technologies should enhance human lives), non-maleficence (cybersecurity technologies should not be used to harm individuals' lives), justice (cybersecurity technologies should improve fairness and provide impartial access for all), autonomy (cybersecurity technologies should not limit users' choices of applications) and explicability (cybersecurity technologies should be both understandable and accountable clearly for their functioning). These principles, along with our reasons for adopting this framework, are described in more detail below.

There is a vulnerability gap related to ethics in cybersecurity, called ethical fading (Bazerman, 2011), that can occur when individuals become oblivious to the ethical implications of a solution by focusing solely on solving the technical aspects of a cybersecurity problem. This can cause a problem for end users. For example, a system administrator who pushes the deployment of two-factor authentication (2FA) on a software application can cause harm (non-maleficence issue) or loss of service (beneficence issue) to vulnerable end users (justice issue) who either have no access to a smartphone or suffer a disability or lack the digital competence needed to use smartphones for 2FA (assuming 2FA is only available via a smartphone's app). Therefore, the system administrator needs to be aware of these ethical implications, and which vulnerable groups are most likely to be impacted, before making final cybersecurity decisions. Though these same general principles will be applicable to a range of computing contexts beyond cybersecurity, our focus here is on the specific ways that these five ethical principles are interpreted and play out in the concrete context of cybersecurity, where there is a vulnerability gap. For most software, the needs of the end user are considered in designing the functionality and usability of the product. This often involves in-depth requirements gathering and understanding of how the user is likely to use the software. However, most cybersecurity software, policies and processes are focused on ensuring privacy and security

and not focused on meeting the specific needs of a target end user of the product or on how users may respond to or be impacted by the security decisions being made. This results in a situation where misalignment is possible, perhaps even probable, between the goals of the cybersecurity professional and the end user, potentially leading to a security breach.

A promising approach to addressing this issue is to educate domain experts more effectively in the ethical issues that arise in cybersecurity. A class of traditional approaches to ethical training focuses on closing the value-action gap (Narvaez, 2005). However, the best way to acquire and practice new skills is to learn by doing through using that skill in action, as this enables learners to understand the problem and how to address it in a range of scenarios (Darcia and Lapsley, 2005). Serious games promise to achieve this goal by providing a safe and engaging virtual environment for role-playing ethically significant scenarios (Hodhod *et al.*, 2009; Staines *et al.*, 2017). We therefore propose the need to develop a serious game for ethical training in cybersecurity contexts.

The overall aim of this study is to build profiles by learning how human factors (e.g personality and values) can influence individuals' ethical decision-making in a serious game based around a cybersecurity context and to explore how to improve ethical awareness in players of that game by leveraging these profiles to later develop artificially intelligent (AI) non-player characters (NPCs) to interact with players (cybersecurity trainees). The purpose of the interaction is to provide the players with a tailored training environment that exposes them to possible human experiences and reactions to cybersecurity technologies and administrative controls and policies that they may (later) be involved in recommending, designing or implementing as cybersecurity domain experts. The goal of achieving tailored training that understands the specific knowledge gaps, biases and tendencies of potential trainees requires a good understanding of what is driving the ethical decision-making of individuals in a cybersecurity context.

To study human values and their influence on cybersecurity decision-making, we utilise Schwartz's theory of basic human values (Schwartz, 1994) as it is commonly used and based on studies of human values across approximately 60 cultures and it identifies 10 universal human values that were later refined to 19 values. To provide our ethical framework, we utilise the principlist approach for cybersecurity ethical decision-making developed by Formosa *et al.* (2021). In this study, we aim to build models that describe the importance of the five principles from that framework (i.e. beneficence, non-maleficence, autonomy, justice and explicability) in different scenarios. We base these models on data collected from studies using earlier prototypes of the serious game, where participants learnt about and had to apply the five principles for cybersecurity ethical decision-making. Our future goal is to use these profiles to build agent-based AI NPCs who encapsulate valid profiles and also adapt their behaviour according to the predicted profile of the player they are interacting with. Drawing on and extending the literature concerning ethical decision-making, we aim to determine which factors are most relevant in influencing cybersecurity ethical decision-making. To create agent profiles and behaviours that plausibly mimic humans, we capture a range of player data including demographics, personality, cyber hygiene practice, knowledge of ethics and moral foundations. Based on players' values, moral stance and individual differences (gender, age, personality and background), we build a descriptive model that we plan to use in the future to provide more tailored and targeted training.

In the following sections, we first present background literature for our work. Section 3 presents our methodology. The results appear in Section 4, followed by discussion, future work and conclusions in Sections 5, 6 and 7, respectively.

2. Background literature

The practice of maintaining a cybersecurity system not only depends on the cybersecurity technologies involved but also on the ethical values that influence human decision-making within that system. Cybersecurity technologies are mainly developed based on the widely

used CIA triad. However, these technologies may raise ethical issues in real-world scenarios (Vallor and Rewak, 2018; Formosa *et al.*, 2021). For example, the possible introduction of 2FA described earlier raised issues related to the ethical principles of non-maleficence, beneficence and justice. In this case, the system administrator needs to be aware of these ethical implications before making any final decision. There is therefore a need to educate professionals and other users of the system, including system architects, administrators and privileged users, about the ethical conflicts and dilemmas that may arise (Blanken-Webb *et al.*, 2018). This education can lead to better moral judgement (Jamal *et al.*, 2016). But to develop those educational resources, we need a relevant ethical framework.

To that end, we leveraged a principlist approach to cybersecurity ethics because it connects cybersecurity to basic ethical concerns. We utilised a framework that has been proposed for the cybersecurity domain by Formosa *et al.* (2021) and which includes five ethical principles: beneficence, non-maleficence, autonomy, justice and explicability. These five ethical principles are modelled on the five AI4People's principles (Floridi *et al.*, 2018) for ethical AI that extends (through the addition of explicability) the same four basic ethical principles developed by Beauchamp and Childress (2001) that are widely accepted in the bioethics domain. The five ethical principles are briefly described below. The reason we selected this ethical framework was that it not only offers a coherent and current framework for cybersecurity ethics based on the literature but it also provides a suitable framework for a pedagogical context. It also helps to keep the range of ethical issues manageable by avoiding the problem of principle proliferation and allows us to move beyond a simplistic focus on privacy by contextualising privacy in terms of a range of differing ethical principles.

Beneficence refers to the opportunity for cybersecurity technologies to enhance individuals' lives. By securing many aspects of activities in day-to-day life, from e-commerce to the private sharing of data, cybersecurity technologies can achieve benefits including promoting human well-being, financial benefits, protecting privacy and strengthening trust. This can shape a safe cybersecurity environment that benefits all. Non-maleficence refers to the importance of cybersecurity technologies not being used to harm individuals. For example, using outdated software as a result of poor cybersecurity practice can harm users of a system by exposing them to vulnerabilities and threats that could compromise their data, cause financial harm and consequently reduce their emotional health and well-being. Autonomy refers to the importance of cybersecurity technologies being developed and deployed in ways that do not unduly limit users' informed choices about how they use that technology. Users, where appropriate, should be given some control to select and manage their own cybersecurity solutions. Failing to obtain informed users' consent for accessing their data also amounts to a failure to respect users' autonomy. Justice refers to the requirement that cybersecurity technologies should improve fairness and provide equitable access for all, while avoiding bias, exploiting the vulnerable and undermining solidarity. For example, designing crucial cybersecurity technologies that are not accessible or useable by members of important social groups, such as the elderly or those with special needs, raises important justice concerns. Likewise, deploying machine learning algorithms trained on deeply biased datasets in cybersecurity contexts risks exacerbating bias and unfairness. Finally, explicability refers to the importance of cybersecurity technologies being both clearly understandable and having clear lines of accountability for their functioning. To achieve this, cybersecurity technologies, for instance, should have a clear definition about responsibility to protect the system and data and how to comply with the responsible use of AI for cybersecurity. Cybersecurity professionals also have responsibilities to maintain and upgrade their professional skills and knowledge, including around the ethical ramifications of the technology.

In a white paper by Yaghmaei *et al.* (2017), it was found that people even from the same culture may perceive ethical values differently in cybersecurity contexts depending on their

professional background. Therefore, it is essential to identify key individual differences in this context. The literature also identifies a problem related to the gap between people's attitudes and ethical intentions (Buchan, 2005). That is, people's ethical values in a cybersecurity context may not match their ethical choices. However, there is a body of research that shows that ethical training can improve ethical decision-making and help to close this gap (Geiger and O'Connell, 1998; Stead *et al.*, 1990; Luthar and Karri, 2005; Cagle and Baucus, 2006). In order to study the link between personal values and ethical behaviour, Mubako *et al.* (2020) conducted an experiment. They focused on the problem of how personal values, using Schwartz' personal value scales, relate to ethical behaviour and explored how ethics training as well as gender and religiosity influence the ethical behaviour of accountants. They collected data via an online survey from 252 accountant undergraduate students from a university in the USA. They hypothesised that Schwartz' personal value scale of openness to change, self-enhancement, conservation and self-transcendence behaviour, as well as ethics training, gender and religiosity all influence ethical behaviour. They created six measures to capture personal use, passing blame, bribery, falsification, padding expenses and deception to evaluate the likelihood of participants engaging in unethical behaviour. Their results show that personal values have a significant effect on ethical behaviour and that conservation and self-transcendence were negatively associated with unethical behaviour. However, openness to change did not influence ethical behaviour. The results also suggest that the likelihood of females engaging in unethical behaviour is lower than males; however, they did not find any meaningful relation between religiosity and ethical behaviour, which they found to be consistent with the literature. Of particular interest to our study, they found that students who reported taking more courses with an ethical component are less likely to be engaged in unethical behaviour (Mubako *et al.*, 2020). This difference in behaviour could be due to the ethics education received in these courses or it could be that more ethically sensitive students choose units with ethics components. In addition, there is evidence in the literature that reminding people about morality may decrease dishonest behaviours (Gino *et al.*, 2009). Gino *et al.* conducted research to argue that there is a link between active social norms and an individual's reaction to unethical behaviour. Individuals and wider social norms play a crucial role in factors influencing decision-making; therefore, it is essential to study those factors given our concern here for cybersecurity ethical decision-making.

A novel study by Ameen *et al.* (2020) focused on the differences between female and male cybersecurity behaviours when using their personal electronic devices, such as a smartphones or tablets, for work as part of a bring-your-own-device (BYOD) policy. Ameen *et al.* (2020) note that while such a policy has obvious benefits, it is also one of the top security risks for companies. They conducted an experiment with the group with the highest use of BYOD from USA (Boston) and United Arab Emirates (UAE) (Dubai) companies. They found significant gender differences in both countries in smartphone security behavioural intentions. The study shows that males and females in both target countries may not be aware of their company's recommendations and policies nor of the security-related risks arising from using their smartphones for work and personal purposes. It also shows that the perceived severity of sanction has a significant effect on males rather than females in the UAE but on both groups in the USA.

The aforementioned studies emphasise that human factors, including demographic information, human values and moral stance, play a crucial role in driving human decision-making in cybersecurity contexts. In the following Table 1, we present a summary of the factors that have been generally found to influence ethical decision-making identified in the above discussed literature and other related studies. Further, given our focus on ethical decision-making, we draw on this table to devise our data collection approach below to evaluate their relevance in a cybersecurity context.

Personality	Big five personality traits (Craft, 2012)
Demographic information	Gender, cultural background and age (Nguyen *et al.*, 2008; Ameen *et al.*, 2020; Herington and Weaven, 2008; Elango *et al.*, 2010; Sweeney *et al.*, 2010; Valentine and Bateman, 2011); the five dimensions of Hofstede (Lu *et al.*, 1999)
Human values	Schwartz's human values (Fritzsche and Oz, 2007)
Moral stance	Reminding people of moral behaviour; credibility and peer influence (i.e. micro-component) (Gino *et al.*, 2009) Stress (Selart and Johansen, 2010), perseverance and self-monitoring (Whitty *et al.*, 2015) Ethical training: (Geiger and O'Connell, 1998), (Stead *et al.*, 1990), (Luthar and Karri, 2005), (Cagle and Baucus, 2006); locus of control: (Whitty *et al.*, 2015); Machiavellian traits, self-control (Craft, 2012); mindfulness (Ruedy and Schweitzer, 2011); attitudes (Buchan (2005)
Other	The supervisor–subordinate and organisational commitment (Liu *et al.* (2020)

Source(s): Table by authors

Table 1.
A summary of identified factors influencing ethical decision-making

3. Methodology

The literature identified a number of human factors that influence cybersecurity ethical decision-making. Our study aims to use the cybersecurity principlist framework (Formosa *et al.*, 2021) described above to identify a connection between these human factors and ethical reasoning in cybersecurity situations, which leads to our study's research question:

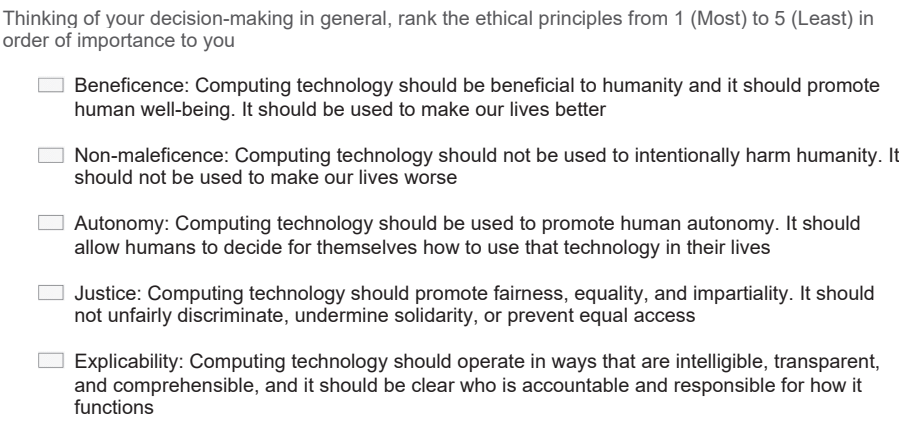
RQ. To what extent do an individual's demographics and other human factors (including personality, moral stance and values) relate to the way they prioritise ethical principles in a cybersecurity context?

By understanding this connection through a serious scenario-based video game, we can help the player to become aware of the relevance of ethical principles in cybersecurity decision-making, reflect on their own reasoning and values in this process and adapt training to ensure the individual is made aware of other viewpoints. To answer our research question, we conducted an online study approved by our University's Human Ethics Research Committee as described in the following sub-sections.

3.1 Study design

To first educate participants about ethical issues in cybersecurity, we designed a serious game to teach players about the five ethical principles described earlier, expose them to ethical cybersecurity decision-making dilemmas and capture data about each player (for further details of the game see Ryan *et al.*, 2022). This data will then be used to build models connecting player profiles with the relative importance they attach to each of the five ethical principles. The game was designed to emulate some common cybersecurity decisions faced by a cybersecurity professional, as well as including other common daily activities, such as an email request to contribute to a colleague's birthday gift, that might arise in an office environment.

The link to the online game was embedded in an online survey. After providing information about the study and acquiring consent for their data to be used, the survey captured basic demographics (e.g. age, gender, cultural background), as well as knowledge of information technology (IT) and ethics, and personality traits. Participants then played the game (described further in the materials section). After playing the game, participants ranked the five ethical principles in order of general importance to them (see Figure 1), and then indicated their moral stance and their values. This allowed us to build a descriptive model of the importance of each of these principles based on the other data.



Source(s): Figure by authors

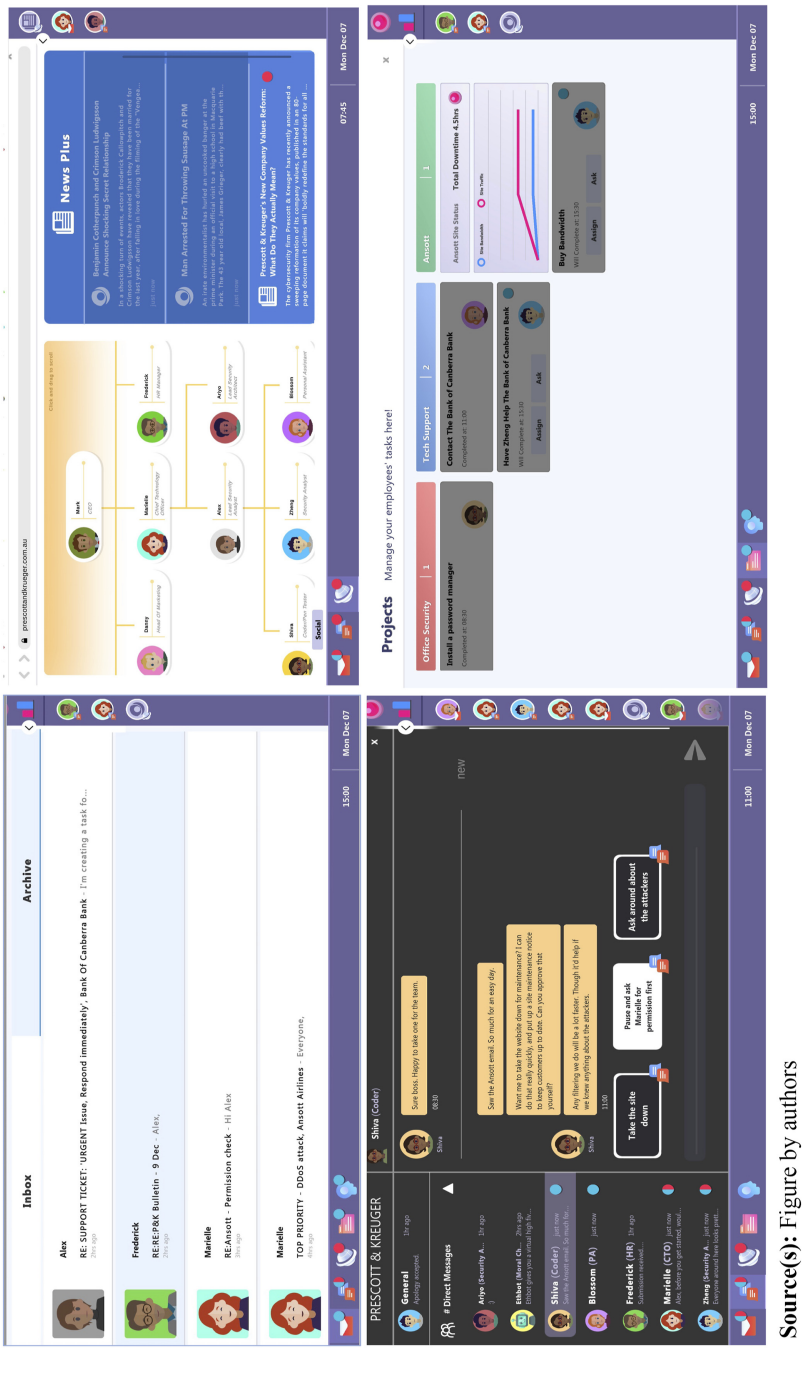
Figure 1.
A snapshot of the five ethical principle ranking choices

3.2 The game

We designed a choice-based narrative game involving interaction with NPCs, most of them playing cybersecurity roles, that simulated a desktop office environment in a fictitious organisation. The game-flow structure was underpinned by Rest's four stage model: moral focus, sensitivity, judgement and action (Jones, 1991). The game was designed to teach participants about ethical issues in cybersecurity and educate them about the five ethical principles in our chosen framework. Raising players' awareness of the five ethical principles and sensitising them to how they are relevant in cybersecurity decision-making was to be achieved by exposing them to different ethical dilemmas in cybersecurity contexts. The scenarios were designed by drawing on real-world cases which were situated within the context of an organisation. To develop in-game scenarios that expose players to a range of cybersecurity techniques and vulnerabilities, we identified key cases reported in the literature which included: DOS (denial of service) and DDOS (distributed denial of service) attacks, ransomware, penetration testing (including white, black and grey hat hacking and bug bounties) and system administration (including managing security and network settings and formulating and policing information and communication technology (ICT) policies). The game was implemented as a web-based application.

Within the game, participants were able to explore various aspects of the simulated organisation by interacting with simplified representations of the activities of email, project management, social media and other applications on the player character's simulated desktop, as shown in Figure 2. The game was designed this way so that information was coming through multiple channels to simulate the way real-world cybersecurity professionals might multi-task across multiple applications and also to challenge the player in relation to certain learning goals (e.g. maintaining moral focus amidst distractions). The player received a training induction to the organisation and the five ethical principles that had been adopted by the organisation.

The player took on the role of a new employee, named Alex, in the position of Lead Security Analyst (Figure 2 top right screen). The player was given a mid-level role in the organisation to facilitate their autonomy in decision-making. Players were given various pre-written options to select from to respond to communications (Figure 2, bottom left screen). The game was comprised of two main interfaces: first, a scripted narrative system using conversations with NPCs and, second, a resource management system to manage the player's and their team's time and other resources (such as bandwidth). Furthermore, the game made



Source(s): Figure by authors

Figure 2.
Screenshots of the playable game

it clear for players that we are looking at the relative importance of the five ethical principles in specific cybersecurity scenarios. For instance, the player had to decide whether they should force pushing installation of a security patch on all employees' machines who failed to do so after several notifications. The possible relative importance of the five ethical principles here include securing the system (beneficence); the potential harm/risk this may cause, such as some users losing access to certain services (non-maleficence); the failure to acquire end-user consent (autonomy); inequalities in who will be most impacted by any action (justice) and the lack of transparency around any forced updates (explicability).

3.3 Sample

The study was conducted in the final week of the first semester of 2021 during a scheduled class. Our participants were university students studying a first-year cybersecurity unit. Students voluntarily consented to allow their data to be used for research purposes. We recruited 366 students. Of the participants, 318 gave consent to use their data. Therefore, we excluded the remaining 48 participants from further analysis. However, only 250 played the game and gave valid responses. We consider responses to be valid if participants did not choose the same option for all questions in each section. Of 244 that identified with binary gender, male was a significant majority over female (190:54). However, we used a sample size with 216 records out of 250 for the classification model. The reason we only used 216 records for the analysis is that sampling for the target variable (the most important principles of the five ethics principles) received only 220 responses in the validated group of 250, and we further removed four of the 220 responses as the same answer were selected for all options.

3.4 Data collection and analysis

We used the Qualtrics Online Survey Platform to collect participants' data. The study was designed to ensure all participants had a similar experience. All students received the same survey questions and game scenarios and had the same amount of time to play the game during the class. All students participated in the study during their scheduled class and interacted with the survey and game online.

To analyse the data, we prepared the data and produced descriptive statistics using Microsoft Excel. Due to gender-based differences in ethical decision-making identified in the literature, we analysed our data using independent *t*-tests to determine any significant differences in the mean responses based on gender. Pearson correlation coefficients analysis was performed to test correlation between the constructs. Cronbach's alpha, Omega and greatest lower bound of reliability were used to test instrument reliability. We used C5.0 classification modelling in IBM SPSS Modeler 18.22 to build decision trees that could be used in the future by our NPCs to reason. Unlike newer machine learning methods, C5.0 produces models that are easier to understand and deploy. We further selected C5.0 due to its higher performance compared to other algorithms available in SPSS. C5.0 is a widely used classification algorithm that uses entropy to split and prune the data to deliver one of the most reliable "out of the box" classifiers based on the tested set of methods (EntezariMaleki *et al.*, 2009; Salzberg, 1994, Han *et al.*, 2011). For this reason, it has become an industry standard. We used the 10-fold cross validation method.

In total we created six models using the principle ranking data shown in Figure 1 to specify the target class: one that predicts which principle will be ranked first and five models, one for each ethical principle, to learn the participants' profiles to predict the ranking for each specific ethical principle. To build the first decision tree, we created a new variable as a target variable (i.e. most-important-principle). We set values for the target variable from 1 to 5 to represent beneficence, non-maleficence, autonomy, justice and explicability, respectively, based on the principle ranked first by the player. For instance, if a person selected beneficence

as the most important principle when making decisions, then we put 1, but if they chose non-maleficence as the most important, we put 2, and so on for all other values. To build the five principle specific models, the target variable is the ranking given for that principle. The purpose of creating five separate principle models is to learn what features of the participants' profile (i.e. moral stance, personality traits and so on) predict their ranking (1–5) for that specific principle. This sheds light on what features are important to capture before or in the game to be able to predict a player's prioritisation of a specific principle. There was a total of 34 input variables (TIPI (5) + Moral Foundations Questionnaire (MFQ) (5) + Schwartz (19) + gender, age, culture, knowledge about ethics and how long playing video games) included in the model. The target variable was each of the five ethical principles per model.

To analyse participants' self-evaluation of knowledge about ethics, we used a six-point Likert scale (0 = I don't want to answer 1 = Terrible, 2 = Poor, 3 = Average, 4 = Good and 5 = Excellent) in which the zero answers were excluded from the calculation.

To capture personality we used the ten-item personality inventory (TIPI) (Gosling *et al.*, 2003). TIPI is a short evaluation form of the big five personality dimensions comprised of 10 items, two for each of the big five factor (BFF) personality dimensions: openness to experience, conscientiousness, extraversion, agreeableness and emotional stability (also known as neuroticism when referred to as the Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism (OCEAN) model), that use a seven-point Likert scale (1 = strongly disagree; 7 = strongly agree), with half of the items reverse coded.

To capture moral stance, the MFQ (Graham *et al.*, 2011) includes two sections with 22 questions in total. It was designed to measure MFQ using a six-point Likert scale (0 = not at all relevant; 5 = extremely relevant) for the first 10 items and from 0 (strongly disagree) to 5 (strongly agree) for the last 10 items. The four items for each five MFQ subscales are totalled to get values in a 0–20 interval. The MFQ includes two unscored items, called Math and Good that are used to test the reliability of the given responses (Graham *et al.*, 2011).

To capture human values, the Portrait Value Questionnaire (PVQ) is based on Schwartz *et al.* (2012)'s 10 basic individual values that influence human actions. It was designed to measure PVQ using a six-point Likert scale (1 = not like me at all, 6 = very much like me). We used PVQ-RR which identifies 19 values comprised from 57 items, where three questions from the PVQ scores are averaged (Schwartz and Butenko, 2014; Schwartz *et al.*, 2001, 2012). PVQ is a strong base for self-evaluation and is suitable for a wide range of ages from different demographic settings (Davidov *et al.*, 2008). Given its broad acceptability, PVQ is considered a strong alternative to the Schwartz value survey (SVS) (Schwartz *et al.*, 2012).

4. Results and findings

To check the data reliability, we ran the Cronbach's alpha test for each of the constructs. The results are as follows: TIPI (0.4527), MFQ (0.8745) and PVQ (0.9743), which categorises the PVQ dataset as Excellent and MFQ as Good in terms of internal consistency. The low result on the Cronbach's alpha for TIPI is expected for this construct. According to Gosling *et al.* (2003), TIPI performs poorly in terms of Cronbach's alpha and confirmatory factor analysis (CFA) or exploratory factor analysis (EFA) indices. This is because it was designed to be a very brief instrument for validity. Deng and Chan (2017) suggest that coefficient Omega may be more suitable as Cronbach's alpha relies on four conditions to hold, compared to two conditions for coefficient Omegas. We also ran McDonald's coefficient Omega (McDonald, 1999) (scale's interpretation is same as alpha coefficient) with the following results that confirms the earlier statements: TIPI (0.628), MFQ (0.825) and PVQ (1.000). TIPI is still low but closer to the 0.70 cut-off for Good. In the long term, our aim is to find minimal measures for personality and values and thus TIPI aligns with this goal, unlike longer versions. TIPI has been found to deliver comparable results for convergence with self and observer ratings,

test–retest reliability and predicted external correlate patterns (Gosling *et al.*, 2003) with the 44 item big five inventory (John and Srivastava, 1999), which is comparable to the 50-item International Personality Item Pool (IPIP) (Goldberg, 1993). However, to further analyse data reliability, we also ran the greatest lower bound of reliability (Woodhouse and Jackson, 1977) via Bayesian single test (Pfadt *et al.*, 2023) and results offer good (>0.7) and excellent (>0.9) reliability as follows; TIPI (0.736), MFQ (0.917) and PVQ (1.000).

4.1 Participants' demographic analysis

Participants were 50 females and 160 males and 6 persons who selected other options for gender. Participants were aged from 17 to 34 year old, with an average age of 19.76 and SD 2.97. Table 2 presents the cultural groups to which participants identified. The participant's knowledge about ethics ranged from 1 to 5 (1 = Terrible, 2 = Poor, 3 = Average, 4 = Good and 5 = Excellent) (mean 3.68; SD 0.74). Participants reported playing video games for 2.89 h on average per week. Computing was the main area of study for participants 71.30% (154/216), followed by business 13.43% (29/216). The other main area of study 8.80% (19/216) included people doing double degrees combining both computing and business as well as related areas of study. Personality, moral stance and Schwartz's human values are presented in Table 3 and Table 4 respectively.

Independent *t*-tests to identify any gender-based differences in our population were performed. Table 5 summarises the only significant differences found between males and females. No other gender differences were statistically significant. Since we are looking at predicting how people prioritise the five principles after learning about and applying them through playing the serious game, we are exploring the influence of demographics, personality, values and moral foundations. Thus, we present unadjusted *p*-values in the paper

The cultural groups	Total	Percentages (%)
Oceania (including Australian)	111	51.39
Southeast Asian	48	22.22
Southern and Central Asian	14	6.48
Northeast Asian	7	3.24
Northernwestern European	5	2.31
Southerneastern European	5	2.31
North African and Middle Eastern	4	1.85
Sub-Saharan African	4	1.85
People of the Americas	1	0.46
No answer or do not identify	17	7.69
Sum	*216*	*100*

Source(s): Table by authors

Table 2. Cultural group distribution

TIPI (scale 1–7)	μ	SD	MFQ (Sum 0–20)	μ	SD
Extraversion	3.79	1.25	Harm	13.81	3.62
Agreeableness	4.32	0.93	Fairness	14.94	3.24
Conscientiousness	4.58	1.19	Ingroup	10.77	4.06
Emotional stability	4.52	1.16	Authority	11.20	4.25
Openness to experiences	4.73	1.02	Purity	12.32	5.93
			Good	4.15	1.00
			Math	1.24	1.87

Source(s): Table by authors

Table 3. Mean and standard deviation for TIPI and MFQ

Table 4.
Mean and standard deviation for Schwartz human values (PVQ)

PVQ (scale 1–6)	μ	SD	PVQ (scale 1–6)	μ	SD
Self-direction thought	4.59	0.91	Tradition	3.47	1.44
Self-direction action	4.40	0.92	Conformity – rules	4.04	1.28
Stimulation	4.11	1.10	Conformity – interpersonal	3.93	1.22
Hedonism	4.45	0.98	Humility	4.18	1.05
Achievement	4.27	1.02	Benevolence –dependability	4.99	0.99
Power dominance	3.73	1.28	Benevolence – caring	4.54	0.94
Power resources	3.51	1.15	Universalism – concern	4.45	1.02
Face	3.93	1.12	Universalism – nature	3.99	1.13
Security personal	4.31	0.98	Universalism –tolerance	4.49	1.01
Security societal	4.07	1.19			

Note(s): *PVQ 1(Not like me at all) – 6 (Very much like me)
Source(s): Table by authors

Table 5.
The significant gender difference results for TIPI, MFQ and PVQ

	Males		Females		Total		
Scales	M	SD	μ	SD	μ	SD	p-value
Ingroup (MFQ)	11.22	4.13	9.36	4.27	10.77	4.06	0.009
Emotional stability (TIPI)	4.6	1.19	4.25	1.04	4.52	1.16	0.03
Universalism – nature (PVQ)	3.83	1.07	4.53	1.26	3.99	1.13	0.03

Source(s): Table by authors

to avoid the likelihood of type II errors that can occur when using Bonferroni adjustments (Perneger, 1998). Unadjusted p-values help us consider what to investigate in the future including what data to capture about players before or during the game.

4.2 Models based on the five ethics principles

As described in section 3.4, in total we created six models, one to predict first ranking and five to predict the ranking of each specific principle. The most significant factors from the model predicting which of the five principles will be ranked first are shown in Table 6. As shown, the main cultural group is the most important predictor with a value of 0.36 (i.e. this variable predicts 36% of the target class) followed by extraversion, conscientiousness and "how many hours per week do you play computer games on average.

Table 7 shows the number of times and the percentage that each principle was ranked first and includes the accuracy of the C5.0 model produced. For example, the largest group of participants (30.55%) considered beneficence the most important ethical principle when making ethical decisions in the cybersecurity domain. Given that there are five principles, there is a 20% chance of randomly selecting the right class. Thus, accuracy rates above 20%

Table 6.
Salient factors that differentiate between the most important principle

Main cultural group	0.3565	Humility	0.0313
Extraversion	0.1966	Authority	0.0283
Conscientiousness	0.1108	Purity	0.0133
Play computer games	0.0980	Self-direction action	0.0133
How old are you	0.0805	Knowledge about ethics	0.0133
Ingroup	0.0472	Stimulation	0.0109

Source(s): Table by authors

are better than chance and are achieved for all five principles. We note that where there are fewer cases (i.e. fewer people ranked that principle first), accuracy is poorer.

Figure 3 aggregates the five principle-specific models. Cultural background, agreeableness, conscientiousness and ingroup are predictors of rankings for all five principles to varying levels of importance. Other features are important only for predicting some or no principles.

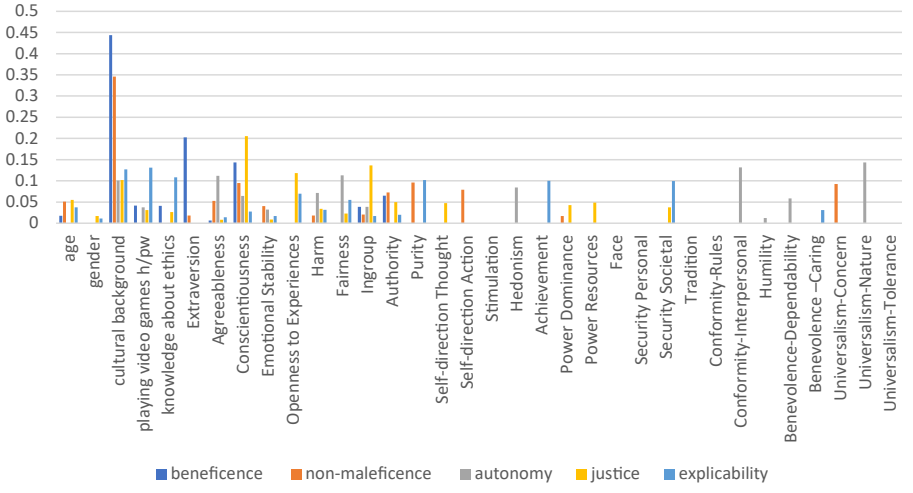
Table 8 presents a brief snapshot of the generated rules (one rule for each ethical principle) to demonstrate how the rules generated use (a subset of) the features in Figure 3 to group (i.e. classify) players who value the same ethical principles highest and differentiate players who value most a different ethical principle. The model is built with 57.87% accuracy. The snapshot is a filter of the full list based on the rules that cover more than three people and/or have high accuracy.

What is apparent in Table 8 is the split between justice and the other four principles based on TIPI conscientiousness, where 6.75 means very high conscientiousness on a seven-point Likert scale, and MFQ ingroup, where 15.5 indicates the top quadrant. The rules also identify a number of other features. We can use the decision tree produced by C5.0 to understand the split according to the values of different features. Table 9 summarises two nodes of the

Ethical principle	Number of times ranked first	Percentage of times ranked first	Accurately classified
Beneficence (1)	66	30.55%	89.39%
Non-maleficence (2)	56	25.92%	46.43%
Autonomy (3)	27	12.50%	37.04%
Justice (4)	44	20.37%	54.55%
Explicability (5)	23	10.26%	26.09%
Total	216	100%	–

Source(s): Table by authors

Table 7. The distribution of first-ranked principles and accuracy



Source(s): Figure by authors

Figure 3. Predictor importance for the five ethical principles

Table 8.
Extracted rules from the model to predict the most important principle

Preferred ethical principle	Conscient-iousness	Ingroup	Cultural background	Play video game	Extraversion	Self-direction thought	Cases/ Coverage	Accuracy
Non-maleficence	≤ 6.75	≤ 15.50	2,3,4,10	–	–		26.142	50.30%
Beneficence	≤ 6.75	≤ 15.50	1	>1.5 h	≤5.25		72.38	38.7%
Autonomy	≤ 6.75	≤ 15.50	5	–	–		3.66	70%
Explicability	≤ 6.75	≤ 15.50	–	>1.5 h	>5.2.5	>4.83	3	100%
Justice	>6.75	–	–	≤3 h	–		5	100%

Note(s): Cultural background: 1 = Oceania (including Australian), 2 = Northernwestern European, 3 = Southerneastern European, 4 = North African or Middle Eastern, 5 = Southeast Asian and 10 = Participants who did not want identify themselves or did not answer
Source(s): Table by authors

decision tree (Nodes 4 and 38) at level three of the tree where we can see the breakdown for cases which met the conditions (Conscientiousness ≤ 6.75 – level 1), (Ingroup ≤ 15.5 – level 2) and split further by culture (level 3) for the two top populated cultural groups: Oceania representing 46.08% and Southeast Asian representing 17.69% of the 216 included records.

5. Discussion

We sought to determine if models could be uncovered to predict, based on individual factors, the importance to participants of our five ethical principles in the context of cybersecurity decision-making. To ensure that they understood these principles and how to apply them to cybersecurity contexts, our participants first played a serious game designed to achieve this outcome before we captured their rankings of the five principles after they played the game. Without playing the game, participants may not have understood the ethical principles or how they apply to cybersecurity. Further, requiring participants to apply the ethical principles enhances their understanding and internalisation of the principles. Explicit reflection activities within the game also aimed to make participants aware of what principles were driving their choices, thereby enabling them to better assess the most important ethical principles to them. Addressing our research question, we now unpack our results to consider the extent to which an individual's demographics and other human factors (including personality, moral stance and values) relate to the way they prioritise ethical principles in a cybersecurity context.

One of the C5.0 models created sought to predict which ethical principle was deemed, in general, to be the most important one based on participants' features. The classification model identified that 77% of the data could be predicted by the main cultural group variable, the personality factors of extraversion and conscientiousness and the number of hours they play video games. The remaining predictors included age, MFQ ingroup and authority, PVQ humility, "knowledge about ethics in IT" and PVQ self-direction action. Some of these findings are confirmed in the literature and some provide new insights.

In their study to predict preferences from individuals' digital behaviour, Kalimeri *et al.* (2019) confirms the role of loyalty/ingroup that accounted for 63% of their study's prediction score and found that Schwartz's human values (conservation and universalism) were the most accurate predictors in their study. Regarding personality traits as predictors for ethical behaviour, Kalshoven *et al.* (2011) found that emotional stability was positively related with ethical leadership. Our model revealed that participants who play computer games more than 1.5 h per week and identified as Oceania prioritise beneficence, suggesting cybersecurity technologies should promote human well-being. Following Jeske and van Schaik (2017) who show that familiarity with threats can mediate Internet attitudes and security behaviours, our finding that previous video gaming experience which constitutes familiarity with a technology (e.g. video games) could mediate ethical decision-making behaviours in cybersecurity contexts that are simulated via a video game.

	Oceania (node 4)		Southeast Asian (node 23)	
Ethical principle	*N*	%	*N*	%
Beneficence	30	30.138	15	30.259
Non-maleficence	25	24.654	6	16.247
Autonomy	19	19.088	4	10.469
Justice	12	12.055	7	18.321
Explicability	14	14.065	6	15.704
Total	100	46.084% of total nodes	38	17.689% of total nodes

Source(s): Table by authors

Table 9. Two decision-tree nodes from the model to predict the most important principle

Lu *et al.* (1999) also found that cultural difference (e.g. western vs eastern culture) may influence ethical decision-making within Hofstede's (Hofstede, 1984) cultural framework. Their findings indicate that US participants are more individualistic and masculine, while Taiwanese participants are more collectivist, less masculine, and have adopted Confucian principles to a greater degree. Their study also confirms that Taiwanese participants demonstrated a stronger preference for rules and regulations than US participants and that this can limit uncertainty in the workplace. Although our study does not focus on Taiwanese vs US participants, we also found cultural difference is predictive. Similarly, a study by Ameen *et al.* (2020) show that female participants in both the US and the UAE countries are more affected by the nature of culture around them in their behavioural intention towards smartphone security. For instance, our study also shows participants belonging to the following three cultural groups, Northernwestern European, Southerneastern European, North African and Middle Eastern, have the same preferences (ranked non-maleficence as the most important ethical principle) when facing ethical dilemmas in terms of our five principles, and they mainly think that cybersecurity technologies should not be used to harm anyone (non-maleficence).

The aggregated models for each of the five principles presented in Figure 3 also confirm that cultural background is the most important predictor for three (i.e. beneficence, non-maleficence and explicability) out of the five ethical principles. Schwartz's universalism nature scale is the most important predictor for autonomy, followed by Conformity – interpersonal, fairness and agreeableness, with the cultural background making very little difference. The most important predictor for justice is TIPI conscientiousness scale followed by ingroup and openness to experiences, with the cultural background again making very little difference. In the combined model to find the first ranked principle, the rule snapshot in Table 8 shows that for our participants high conscientiousness (>6.75) was only an important predictor for justice, in comparison to the other four principles where lower conscientiousness was an important predictor. Given the focus of high conscientiousness personality types on adhering to norms and rules, a close association of this trait with the principle of justice is not surprising (Fu and Lihua, 2012; Rice *et al.*, 2020).

Our study sought to investigate the role that personal values might play in influencing ethical decision-making in cybersecurity. Figure 3 shows that 13 of Schwartz's 19 values are predictors of importance, but only 2 influence more than one principle and none predict beneficence. As explained earlier, our aim is to use these models to build AI NPCs with plausible profiles who can predict the ethical priorities (and biases) of the player. The ultimate aim is to tailor the training simulation so that the player becomes sensitised to other viewpoints and the potential ramifications of their cybersecurity decisions and actions concerning the policies, processes and technologies they propose and implement. From a practical perspective, we are seeking to address the situation where, for example, as system administrators, they might choose to force the release of an ethical worm to install security patches to limit harm to users (prioritising non-maleficence), but fail to acquire the consent (autonomy), respect the ownership rights (justice) of users or properly explain (explicability) their actions (Formosa *et al.*, 2021). To that end, before or while playing the game any feature used to predict the players' priorities would need to be captured. This means, we need to minimise how many features are included in our models. Given that many of Schwartz's values are important for only one principle, there may be little value to capturing Schwartz's values by asking 57 questions. We note, however, that for Justice, the two most important features are Schwartz's values. In implementing the models in our game, we will be identifying which features are of most value and ensure that all five principles can be predicted. The results reported here, and our full model not reported due to space and complexity (full models available by request from the authors), provide us with this valuable information.

Regarding the influence of personality, Table 6 and Figure 3 reveal that all five personality dimensions influence the importance of different ethical principles. Table 6 shows extraversion as the next biggest predictor after culture. Gratian *et al.* (2018) suggested that extraversion is a significant predictor of good device securement behavioural intentions. However, we see in Figure 3 that extraversion only predicts beneficence and non-maleficence to a much lower extent. Conscientiousness is a predictor for all five principles, confirmed further in the rules in Table 8. We can see considerable support in the literature for the influence of personality on decision-making. Özbağ (2016) observed that agreeableness, conscientiousness and openness to experience are positively linked to actions of ethical leadership. Their findings, however, did not confirm any significant link between extraversion and ethical leadership.

Looking at Figure 3, age was a factor for all principles except autonomy. Looking at the rules (not reported here), the split is around 18.5 year old, where participants younger than 19 year old on average prioritise non-maleficence, suggesting that they focus on the harm minimisation aspects of cybersecurity technologies, while those who are older than 19 year old prioritise beneficence, suggesting that they focus more on the potential benefits of cybersecurity technologies rather than avoiding harms. Age has been found to impact ethical decision-making in other studies. A study by Elango *et al.* (2010), for example, shows that older managers (above 35 year old) were more likely to make ethical choices based on their own values, while younger managers (below 35 year old) were more likely to be influenced by organizational ethics.

The C5.0 decision trees identified that MFQ subscales are another important factor. The ingroup subscale was a feature included in most rules predicting the importance of a principle. Commonly the rule condition used the value of <15.5, which is higher than the mean MFQ score of 10.77. This cut-off indicates that those who scored above 15.5 for ingroup were less driven by ethical principles and more inclined to put the interests of their ingroup above their ethical concerns for others. Chowdhury (2017) also found that loyalty/ingroup was positively associated with unethical consumer actions and negatively associated with perceptions of prosocial consumer actions. These findings suggest that for individuals who highly value their ingroup, it may be important to use strategies, such as our proposed game, to identify and highlight the impact of their ethical choices on those outside their ingroup. A study by Kalimeri *et al.* (2019) also note the need to do more research about the role of human values and morality in predicting personality and human values from digital behaviours.

While gender differences in ethical behaviour have been widely identified in the literature (Elango *et al.*, 2010; Herington and Weaven, 2008; Nguyen *et al.*, 2008; Sweeney *et al.*, 2010; Valentine and Bateman, 2011), gender was not a salient factor in our machine learning models or our statistical analyses, with the exception of TIPI – emotional stability, MFQ – ingroup and PVQ – universalism – nature. Interestingly, each of these significantly different features appeared in our models, with ingroup being the most salient feature of the three. The salience of these features in identifying principle importance may reflect a gender difference. Since C5.0 uses information gain to split the data, it discards attributes not needed for splitting. Thus, gender may have been discarded resulting in minimal influence in the models. Another reason may be the gender imbalance in our sample population, with a majority of males to females (190:54). This gender imbalance, however, is representative and consistent with the imbalance observed in the unit participants were recruited from and among professionals in the ICT/cybersecurity industry.

6. Implications

Overall, our study has provided a first attempt to model, after ethical training by playing a serious game, the connection between the importance of ethical principles for cybersecurity

decision-making and the demographic, personality and ethical profiles of individuals. This has important practical implications as it helps us to understand and predict how people may choose to prioritise competing ethical concerns when they conflict with one another in cybersecurity contexts. While further data collection and analyses are required to build more accurate descriptive models, we suggest an initial generalised model of the rules as presented in Table 6. It is clear that individuals prioritise different ethical principles. While approx. 56% of participants were most concerned with delivery of the potential benefits of cybersecurity technologies (30.55%) e.g. data protection) or the avoidance of harm (25.92% e.g. data loss or breach), those prioritising justice want cybersecurity technologies to be fair and not to perpetuate bias and injustice (including in terms of accessibility). The low percentage of players prioritising autonomy (12.5%), which values asking for consent and allowing users to make their own cybersecurity choices, is somewhat surprising if we contrast autonomy's high importance in ethical decision-making in other domains, such as health (Cullati *et al.*, 2011). Loi *et al.* (2019) also identified autonomy as the most important bioethics principle in the health domain and noted that prioritising autonomy can result in conflicts with other bioethics principles. Perhaps one's health behaviours are seen as personal choices that have greater impact on one's life. Whereas in the context of cybersecurity decision-making, choices may not be viewed as being as important and individuals may also feel less equipped to make such decisions due to limited technical expertise. While perhaps not surprising, explicability was ranked as the least important principle by participants' (10.26%). This reveals that concerns around explanations of cybersecurity policy, transparency of cybersecurity decision-making and clarity around accountability for cybersecurity technologies were less important ethical considerations for our participants. The low numbers for autonomy and explicability warrant more data collection to build profiles to model those who prioritise these principles and also suggest ethics training on these principles is needed.

As mentioned in the introduction, the dual motivation for this study, beyond understanding which ethical principles participants prioritise, is to build profiles that could be used to create realistic NPC agents in a serious game. This paper reports our first attempt to explore and learn players' profiles based on their responses to prioritising the five ethical principles in cybersecurity contexts. Once we have learnt and built these profiles, we can better tailor the ethical education in the game for the players (e.g. cybersecurity professionals/students). In other words, our plan is to use the predicted profiles outlined here to identify and target individuals that are less focused on or less aware of specific ethical principle/s and their relevance in cybersecurity contexts and then to expose such individuals to viewpoints and scenarios that they are less likely to consider. For example, if a player has a profile that indicates they are unlikely to prioritise explicability, the scenario they are exposed to in the game could consider issues such as transparency, accountability and responsibility and show how these concerns for some users may result in them making a poor cybersecurity decision or failing to follow policy resulting in a breach. This will help the cybersecurity professional to take these viewpoints and possible behaviours into account in the design and implementation of cybersecurity technologies and policies. A key approach for achieving this is to adapt the responses of the AI NPCs to present to the player alternative viewpoints from those held by the player.

Our approach to model players can be applied to different audiences beyond cybersecurity professionals. The next version of the game could, for example, be designed to include scenarios for end users to help them reflect on their ethical choices in the use of cybersecurity technologies. This will require developing scenarios, such as a ransomware attack on private files, that end users (rather than cybersecurity professionals) could experience. Further investigation along these lines is also warranted to help managers and professionals in the cybersecurity domain better understand the possible behaviours of others in their team and across their organisation, as well as their customers or user base.

7. Limitations and future work

The first limitation of our study is the size of the participant dataset. Although the number of valid records in our dataset (N = 216) is not large enough to generalise any rules with confidence, it is enough to generate insights into how people prioritise ethical principles when facing cybersecurity dilemmas and to indicate areas that warrant further research. The second limitation of our study is that our participants were all university students studying introductory cybersecurity and there was a gender imbalance, with many more males compared to females. For more generalisable results, we would need to extend the study to a wider range of target audiences, including cybersecurity professionals, managers, end users and the broader public. These studies could also seek a greater gender balance in accordance with the profile of the target group. To reach different audiences, we need to change the game scenarios and interactions to be relevant to each audience. It may also be necessary to modify game mechanics to suit the targeted demographic. Finally, using different contexts and scenarios could influence which ethical principles are relevant and important for decision-making. We aim to address this issue in future studies by asking participants to rank their ethical principles in a range of specific contexts rather than in general.

8. Conclusions

Given the importance of understanding the impact of human factors in cybersecurity, the main purpose of this study was to learn what factors influence prioritisation of ethical principles in a cybersecurity domain. To learn the participants' ethical profile in a cybersecurity context, we created a serious game that provided training on five ethical principles relevant to cybersecurity decision-making and then exposed participants to a series of cyberethical dilemmas requiring them to apply those principles. After undertaking this training by playing a serious game, we asked participants to rank the importance in general of the five ethical principles they learnt about and practiced using in the game. We found that their rankings could be predicted primarily based on the order of importance; firstly, by their demographic information (cultural background), then personality dimensions (conscientiousness and extraversion), moral foundations (ingroup, authority and purity), Schwartz's human values (humility, stimulation and self-direction action), knowledge about ethics and video game playtime. Our models also show that cultural background was the greatest predictor for ranking the principles of beneficence, non-maleficence and explicability as the most important principle.

Going forward, we intend to use the profiles uncovered here to build AI NPCs which will simulate and reason about a range of human ethical viewpoints in response to cybersecurity scenarios that unfold within a virtual work environment. Through interaction, the NPCs will expose the player to multiple viewpoints. Based on the player's predicted viewpoint, the NPCs will adapt their training to help the player better understand the possible human responses and factors that can impact cybersecurity designs, implementations and policy decisions. In this way individuals that are predicted, based on their profile, to be less familiar with a specific ethical principle in a cybersecurity context could be provided with targeted interactive ethical education that could help them to make moral judgements that more closely adhere to ethical principles.

Note

1. http://targetedattacks.trendmicro.com/

References

Ameen, N., Tarhini, A., Hussain Shah, M. and Madichie, N.O. (2020), "Employees' behavioural intention to smartphone security: a gender-based, cross-national study", *Computers in Human Behavior*, Vol. 104, pp. 106-184.

Bazerman, M.H. (2011), *Blind Spots: Why We Fail to Do What's Right and what to Do about it*, Unabridged edition, Brilliance Audio, Grand Haven, Michigan.

Beauchamp, T. and Childress, J. (2001), *Principles of Biomedical Ethics*, Oxford University Press, Oxford.

Blanken-Webb, J., Palmer, I., Deshaies, S.-E., Burbules, N.C., Campbell, R.H. and Bashir, M. (2018), "A case study-based cybersecurity ethics curriculum", *2018 (USENIX) Workshop on Advances in Security Education (ASE18)*.

Brey, P. (2007), "Ethical aspects of information security and privacy", in Petković, M. and Jonker, W. (Eds), *Security, Privacy, and Trust in Modern Data Management*, Berlin, Heidelberg, pp. 21-36, Springer Berlin Heidelberg.

Buchan, H.F. (2005), "Ethical decision making in the public accounting profession: an extension of Ajzen's theory of planned behavior", *Journal of Business Ethics*, Vol. 61 No. 2, pp. 165-181.

Cagle, J.A.B. and Baucus, M.S. (2006), "Case studies of ethics scandals: effects on ethical perceptions of finance students", *Journal of Business Ethics*, Vol. 64 No. 3, pp. 213-229.

Chowdhury, R.M.M.I. (2017), "The moral foundations of consumer ethics", *Journal of Business Ethics*, Vol. 158 No. 3, pp. 585-601.

Christen, M., Gordijn, B., Weber, K., van de Poel, I. and Yaghmaei, E. (2017), "A review of value-conflicts in cybersecurity", *The ORBIT Journal*, Vol. 1 No. 1, pp. 1-19.

Craft, J.L. (2012), "A review of the empirical ethical decision-making literature: 2004-2011", *Journal of Business Ethics*, Vol. 117 No. 2, pp. 221-259.

Cullati, S., Courvoisier, D.S., Charvet-Bérard, A.I. and Perneger, T.V. (2011), "Desire for autonomy in health care decisions: a general population survey", *Patient Education Counseling*, Vol. 83 No. 1, pp. 134-138.

Darcia, N. and Lapsley, D.K. (2005), "The psychological foundations of everyday morality and moral expertise", *Character Psychology and Character Education*, pp. 140-165.

Davidov, E., Schmidt, P. and Schwartz, S.H. (2008), "Bringing values back in: the adequacy of the European social survey to measure values in 20 countries", *Public Opinion Quarterly*, Vol. 72 No. 3, pp. 420-445.

Deng, L. and Chan, W. (2017), "Testing the difference between reliability coefficients alpha and Omega", *Educational and Psychological Measurement*, Vol. 77 No. 2, pp. 185-203.

Elango, B., Paul, K., Kundu, S.K. and Paudel, S.K. (2010), "Organizational ethics, individual ethics, and ethical intentions in international decision-making", *Journal of Business Ethics*, Vol. 97 No. 4, pp. 543-561.

EntezariMaleki, R., Rezaei, A. and MinaeiBidgoli, B. (2009), "Comparison of classification methods based on the type of attributes and sample size", *Journal of Convergence Information Technology*, Vol. 4 No. 3, pp. 94-102.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P. and Vayena, E. (2018), "AI4People-An ethical framework for a good AI society: opportunities, risks, principles, and recommendations", *Minds and Machines (Dordr)*, Vol. 28 No. 4, pp. 689-707.

Formosa, P., Wilson, M. and Richards, D. (2021), "A principlist framework for cybersecurity ethics", *Computers and Security*, Vol. 109, 102382.

Fritzsche, D. and Oz, E. (2007), "Personal values' influence on the ethical dimension of decision making", *Journal of Business Ethics*, Vol. 75 No. 4, pp. 335-343.

Fu, Y. and Lihua, Z. (2012), "Organizational justice and perceived organizational support", *Nankai Business Review International*, Vol. 3 No. 2, pp. 145-166.

Gee, J.P. (2007), *What Video Games Have to Teach Us about Learning and Literacy*, Palgrave Macmillan, New York, NY.

Geiger, M.A. and O'Connell, B.T. (1998), "Accounting student ethical perceptions: an analysis of training and gender effects", *Teaching Business Ethics*, Vol. 1, pp. 371-388.

Gino, F., Ayal, S. and Ariely, D. (2009), "Contagion and differentiation in unethical behavior: the effect of one bad apple on the barrel", *Psychological Science*, Vol. 20 No. 3, pp. 393-398.

Goldberg, L.R. (1993), "The structure of phenotypic personality traits", *American Psychologist*, Vol. 48 No. 1, p. 26.

Gosling, S.D., Rentfrow, P.J. and Swann, W.B. (2003), "A very brief measure of the Big-Five personality domains", *Journal of Research in Personality*, Vol. 37 No. 6, pp. 504-528.

Graham, J., Nosek, B.A., Haidt, J., Iyer, R., Koleva, S. and Ditto, P.H. (2011), "Mapping the moral domain", *Journal of Personality and Social Psychology*, Vol. 101 No. 2, pp. 366-385.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A. (2018), "Correlating human traits and cyber security behavior intentions", *Computers and Security*, Vol. 73, pp. 345-358.

Han, J., Pei, J. and Kamber, M. (2011), *Data Mining: Concepts and Techniques*, Elsevier, Burlington, Massachusetts.

Herington, C. and Weaven, S. (2008), "Improving consistency for DIT results using cluster analysis", *Journal of Business Ethics*, Vol. 80 No. 3, pp. 499-514.

Hodhod, R., Kudenko, D. and Cairns, P. (2009), "Serious games to teach ethics", *Adaptive and Emergent Behaviour and Complex Systems - Proceedings of the 23rd Convention of the Society for the Study of Artificial Intelligence and Simulation of Behaviour*, *AISB 2009*, Edinburgh, 6 April 2009, pp. 43-52.

Hofstede, G. (1984), *Culture's Consequences: International Differences in Work Related Values*, Geert Hofstede, Sage Publications, London and Beverly Hills, 1980, p. 475, doi: 10.1002/job.4030030208.

Jamal, A., Ferdoos, A., Zaman, M. and Hussain, M. (2016), "Cyber-ethics and the perceptions of Internet users: a case study of university students of Islamabad", *Pakistan Journal of Information Management and Libraries*, Vol. 16, p. 725.

Jeske, D. and van Schaik, P. (2017), "Familiarity with Internet threats: beyond awareness", *Computers and Security*, Vol. 66, pp. 129-141.

John, O.P. and Srivastava, S. (1999), "The Big-Five trait taxonomy: history, measurement, and theoretical perspectives", in Pervin, L., and John, O. (Eds.), *Handbook of Personality Theory and Research*. Guilford Press, New York.

Jones, T.M. (1991), "Ethical decision making by individuals in organizations: an issue-contingent model", *Academy of Management Review*, Vol. 16 No. 2, pp. 366-395.

Kalimeri, K., Beiró, M.G., Delfino, M., Raleigh, R. and Cattuto, C. (2019), "Predicting demographics, moral foundations, and human values from digital behaviours", *Computers in Human Behavior*, Vol. 92, pp. 428-445.

Kalshoven, K., Den Hartog, D.N. and De Hoogh, A.H.B. (2011), "Ethical leader behavior and big five factors of personality", *Journal of Business Ethics*, Vol. 100 No. 2, pp. 349-366.

Liu, C., Wang, N. and Liang, H. (2020), "Motivating information security policy compliance: the critical role of supervisor-subordinate guanxi and organizational commitment", *International Journal of Information Management*, Vol. 54, 102152.

Loi, M., Christen, M., Kleine, N. and Weber, K. (2019), "Cybersecurity in health–disentangling value tensions", *Journal of Information, Communication Ethics in Society*, Vol. 17 No. 2, pp. 229-245, doi: 10.1108/JICES-12-2018-0095.

Lu, L.C., Rose, G.M. and Blodgett, J.G. (1999), "The effects of cultural dimensions on ethical decision making in marketing: an exploratory study", *Journal of Business Ethics*, No. 18, pp. 91-105.

Luthar, H.K. and Karri, R. (2005), "Exposure to ethics education and the perception of linkage between organizational ethical behavior and business outcomes", *Journal of Business Ethics*, Vol. 61 No. 4, pp. 353-368.

Mann, I. (2008), *Hacking the Human: Social Engineering Techniques and Security Countermeasures*, Routledge, London, p. 266, doi: 10.4324/9781351156882.

McDonald, R.P. (1999), *Test Theory: A Unified Treatment*, Psychology Press, London.

Mubako, G., Bagchi, K., Udo, G. and Marinovic, M. (2020), "Personal values and ethical behavior in accounting students", *Journal of Business Ethics*, Vol. 174, pp. 161-176.

Narvaez, D. (2005), "Integrative ethical education", *Handbook of Moral Development*, Pyschology Press, London.

Nguyen, N.T., Basuray, M.T., Smith, W.P., Kopka, D. and McCulloh, D. (2008), "Moral issues and gender differences in ethical judgment using Reidenbach and Robin's (1990) multidimensional ethics scale: implications in teaching of business ethics", *Journal of Business Ethics*, Vol. 77 No. 4, pp. 417-430.

Nobles, C. (2018), "Botching human factors in cybersecurity in business organizations", *HOLISTICA–Journal of Business and Public Administration*, Vol. 9 No. 3, pp. 71-88.

Özbağ, G.K. (2016), "The role of personality in leadership: five factor personality traits and ethical leadership", *Procedia – Social and Behavioral Sciences*, Vol. 235, pp. 235-242.

Perneger, T.V. (1998), "What's wrong with Bonferroni adjustments", *British Medical Journal*, Vol. 316 No. 7139, pp. 1236-1238.

Pfadt, J.M., Bergh, D.V.D., Sijtsma, K. and Wagenmakers, E.-J. (2023), "A tutorial on Bayesian single-test reliability analysis with JASP", *Behavior Research Methods*, Vol. 55, pp. 1069-1078, doi: 10.3758/s13428-021-01778-0.

Rice, D.B., Young, N.C., Johnson, D., Walton, R. and Stacy, S. (2020), "Overall justice and supervisor conscientiousness: implications for ethical leadership and employee self-esteem", *Business Ethics: A European Review*, Vol. 29 No. 4, pp. 856-869.

Ruedy, N.E. and Schweitzer, M.E. (2011), "In the moment: the effect of mindfulness on ethical decision making", *Journal of Business Ethics*, Vol. 95 No. S1, pp. 73-87.

Ryan, M., McEwan, M., Sansare, V., Formosa, P., Richards, D. and Hitchens, M. (2022), "Design of a serious game for cybersecurity ethics training", *Proceedings of the 2022 Digital Games Research Association (DIGRA) International Conference: Bringing Worlds Together*, July 7–11, 2022, Kraków, Poland, available at: http://www.digra.org/wp-content/uploads/digital-library/DiGRA_2022_paper_156.pdf

Safa, N.S., Von Solms, R. and Futcher, L. (2016), "Human aspects of information security in organisations", *Computer Fraud and Security*, Vol. 2016 No. 2, pp. 15-18.

Salzberg, S.L. (1994), "C4.5: programs for machine learning by J. Ross Quinlan. Morgan Kaufmann publishers, 1993", *Machine Learning*, Vol. 16 No. 3, pp. 235-240.

Schwartz, S.H. (1994), "Are there universal aspects in the structure and contents of human values?", *Journal of Social Issues*, Vol. 50 No. 4, pp. 19-45.

Schwartz, S.H. (2012), "An overview of the Schwartz theory of basic values", *Online Readings in Psychology and Culture*, Vol. 2 No. 1, pp. 2307-0919, 11.

Schwartz, S.H. and Butenko, T. (2014), "Values and behavior: validating the refined value theory in Russia", *European Journal of Social Psychology*, Vol. 44 No. 7, pp. 799-813.

Schwartz, S.H., Melech, G., Lehmann, A., Burgess, S., Harris, M. and Owens, V. (2001), "Extending the cross-cultural validity of the theory of basic human values with a different method of measurement", *Journal of Cross-Cultural Psychology*, Vol. 32 No. 5, pp. 519-542.

Schwartz, S.H., Cieciuch, J., Vecchione, M., Davidov, E., Fischer, R., Beierlein, C., Ramos, A., Verkasalo, M., Lonnqvist, J.E., Demirutku, K., Dirilen-Gumus, O. and Konty, M. (2012), "Refining the theory of basic individual values", *Journal of Personality and Social Psychology*, Vol. 103 No. 4, pp. 663-688.

Selart, M. and Johansen, S.T. (2010), "Ethical decision making in organizations: the role of leadership stress", *Journal of Business Ethics*, Vol. 99 No. 2, pp. 129-143.

Staines, D., Formosa, P. and Ryan, M. (2017), "Morality play: a model for developing games of moral expertise", *Games and Culture*, Vol. 14 No. 4, pp. 410-429.

Stead, W.E., Worrell, D.L. and Stead, J.G. (1990), "An integrative model for understanding and managing ethical behavior in business organizations", *Journal of Business Ethics*, No. 9, pp. 233-242.

Sweeney, B., Arnold, D. and Pierce, B. (2010), "The impact of perceived ethical culture of the firm and demographic variables on auditors' ethical evaluation and intention to act decisions", *Journal of Business Ethics*, Vol. 93 No. 4, pp. 531-551.

Valentine, S.R. and Bateman, C.R. (2011), "The impact of ethical ideologies, moral intensity, and social context on sales-based ethical reasoning", *Journal of Business Ethics*, Vol. 102 No. 1, pp. 155-168.

Vallor, S. and Rewak, W. (2018), *An Introduction to Cybersecurity Ethics*, Markkula Center for Applied Ethics, p. 65, available at: https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf (accessed 10 May 2023).

Whitty, M., Doodson, J., Creese, S. and Hodges, D. (2015), "Individual differences in cyber security behaviors: an examination of who is sharing passwords", *Cyberpsychology, Behavior, and Social Networking*, Vol. 18 No. 1, pp. 3-7.

Woodhouse, B. and Jackson, P.H. (1977), "Lower bounds for the reliability of the total score on a test composed of non-homogeneous items: II: a search procedure to locate the greatest lower bound", *Psychometrika*, Vol. 42 No. 4, pp. 579-591.

Yaghmaei, E., van de Poel, I., Christen, M., Gordijn, B., Kleine, N., Loi, M., Morgan, G. and Weber, K. (2017), "Canvas white paper 1 – cybersecurity and ethics (October 4, 2017)", available at: https://ssrn.com/abstract=3091909, doi: 10.2139/ssrn.3091909.

Corresponding author
Deborah Richards can be contacted at: deborah.richards@mq.edu.au