

Roll With It: Awareness Raising with Cyber Defence Dice

Steven Furnell
School of Computer Science
University of Nottingham
Nottingham, United Kingdom
steven.furnell@nottingham.ac.uk
0000-0003-0984-7542

Lucija Šmid
School of Management
University of Bath
Bath, United Kingdom
ls2793@bath.ac.uk
0009-0004-3119-9312

James Todd
School of Computer Science
University of Nottingham
Nottingham, United Kingdom
james.todd@nottingham.ac.uk
0009-0009-2670-8473

Xavier Carpent
School of Computer Science
University of Nottingham
Nottingham, United Kingdom
xavier.carpent@nottingham.ac.uk
0000-0003-1697-6940

Simon Castle-Green
School of Computer Science
University of Nottingham
Nottingham, United Kingdom
simon.castle-green@nottingham.ac.uk
0000-0003-0681-2555

Abstract—Cybersecurity awareness is widely recognized as an important requirement, but is frequently overlooked or addressed in ways that do not engage the interest of the target audience. In an attempt to broaden the options available for achieving this, the paper discusses the concept, design and evaluation of a new dice-based game designed to promote entry-level cyber security awareness in relation to common forms of attack and defence. The concept of the game is that players can defend against prior attacks, or use attacks to test defences, with the images on the different die faces denoting threats and safeguards of different strengths and which are countered in different ways. The discussion includes a worked example of one of the game modes that has been designed in order to illustrate how players would take turns and make decisions in practice. It then presents initial results from a series of seven hands-on playtest sessions conducted with a range of audiences, including the general public, cyber educators and cyber professionals. The findings indicate that all audiences were positive about the game concept and found it enjoyable to play. Additionally, it was recognized to have value in raising and maintaining awareness, and would be a game that participants would play again and recommend to others.

Keywords—*cyber awareness, cyber engagement, dice, gamification*

I. INTRODUCTION

Cyber security literacy is now an essential requirement for the population at large, but an area in which many still appear unfamiliar and potentially underprepared. For the general public the most common solution is to direct people to a webpage, whereas within organisations the answer tends to be some form of online training. However, in both cases users are generally left to pursue it on their own, and may not find it

an engaging activity. Moreover, in the organisational setting, cybersecurity training is often delivered via the same channel as other organisational learning such as Health and Safety, Equality and Diversity, and Data Protection. While this serves to position cyber security as being of comparable importance to these other issues, and gets the job done from a compliance perspective, it is less likely to be winning hearts and minds or promoting real engagement. This realisation has driven many to conclude that cyber security learning needs to be more interactive and indeed fun. This in turn has given rise to various attempts to create cybersecurity themed games, in both digital and physical formats. While both have clear value, the latter are of particular interest in the context of capturing interest of groups of players and leveraging related social advantages (e.g. for use during security awareness sessions within organizational or academic classes). With this in mind, the paper presents the concept and operation of a new in-person game based on dice, which seeks to support the initial stages of cybersecurity awareness. The next section presents some background context in terms of existing cybersecurity games, leading into the justification for designing the new game, which is then outlined in Section III. The resulting gameplay is then explained in Section IV, including a worked example of how the main version of the game is played. Section V then describes evaluation findings from a series of hands-on playtests, the implications of which are then further discussed in Section VI. The paper concludes with reflections upon the contribution, and an example of how the game has already been extended for those that wish to go beyond the basic implementation.

II. BACKGROUND

Cybersecurity is a popular focus for gamification, and various games have been produced in both digital and physical formats. Digital games can be found in both web and app-

based formats, with an early example of the former being Anti-Phishing Phil, a web-based game that seeks to teach players about suspicious links [1], This now dates back around two decades, and numerous other examples of digital games and gamification have appeared since. Some, such as [2], have focused on the same theme of phishing, while others have tackled other common areas of end-user vulnerability, such as password security [3,4] and USB-based attacks [5]. The formats of the games also vary, from arcade-style games through to role-playing and problem solving. The resulting landscape of digital games is extensive, and further details of the wider breadth can be found in existing review papers such as [6]. However, while such games have the potential to enhance interest and engagement beyond typical online training, a potential downside is that participants are still playing in isolation, and lack the opportunity for discussion and interaction that they would experience in traditional classroom-based contexts. As a result, there have also been significant developments in terms of cybersecurity games in physical formats.

Existing examples of physical/in-person games are most commonly presented in the form of tabletop board games and card games. An extensive summary of prior offerings in this space is presented by Shostack [7], and readers are referred to this source for a full sense of the range and diversity of games that have been produced. However, the following illustrative examples are briefly outlined below in order to give a sense of the some of the more widely-cited games and how they have been realised:

- **Backdoors & Breaches:** A card-based game for two or more players (5-7 recommended), and based on the premise of defending against attack scenarios [8]. The game involves 52 cards, including Attacks (split into four further categories: Initial Compromise, Pivot and Escalate, C2 and Exfil, and Persistence), Procedures and Injects. An 'Incident Captain' builds a scenario from the 4 attack cards) and one or more Defenders then select from Procedure cards in order to try to counter the attack. The game ends if the Defenders successfully reveal all four attack cards, or if ten turns have passed (with overall games lasting 30-60 minutes).
- **Control-Alt-Hack:** A card-based game for 3-6 players, aged 14 and up, where the players work for a white-hat ethical hacking company [9]. The game is focused around Missions, and Hackers with different skills (e.g. cryptanalysis, hardware hacking, social engineering). Completing Missions involves rolling standard numbered dice to determine the skill level required for each task involved, and then determining if your Hacker has the level needed (completing all tasks completes the Mission). Further depth is added through the use of elements such as Entropy cards, and the use of Money and Hacker Cred tokens. Games last around one hour.
- **Cyber Threat Defender:** A two-player competitive collectible card game for ages 11 and up. There are four

types of card: Assets, Defences, Events and Attacks [10]. The game involves producing a network of Assets, and then building Defences that protect them from Attacks. Events are then random occurrences that may be to the benefit or detriment of security. Each card has a name, a description of what it is, a description of its resulting effect, and a points value. Players take turns within rounds, and the first to 30 points wins (or to -45 loses), with an average play time of 20 minutes.

- **Decisions & Disruptions:** A tabletop game (but not in boardgame format) in which players must manage the security of a small utility company. The game is set in the context of industrial control systems security, and uses LEGO pieces to enable players to construct their environment and defences. Players are required to make decisions in relation to threats, vulnerabilities and attacks, working within the constraints of budget limitations [11]. It is designed for 5-8 players plus a Game Master and games can last up to two hours.
- **Riskio:** A tabletop game for 3-5 players, plus a Games Master (who needs to be an experienced cyber professional), which aims to "increase cyber security awareness for people with no technical background working in organisations" [12]. Players must protect the organisation's data and services against various threats (with 78 related cards split across the categories of Spoofing, Tampering, Repudiation, Information Disclosure, Denial of services, and Elevation of Privilege). Games can last around 45 minutes.

While all offer value in terms of cyber security learning, existing games often tend to share one or more of the following characteristics:

- intended as relatively long form engagements, often requiring a non-trivial degree of initial setup and explanation of the rules, with play then expected to last upwards of 20 minutes (and sometimes considerably longer).
- aimed at players who are already somewhat knowledgeable about cybersecurity, or actively interested in learning more about it.
- requiring a facilitator (games master) to run the session, which adds to the level of prior planning and organisation involved in playing the game.

While these may be fine for a pre-planned awareness and training session, the games consequently lend themselves less well to quick use in more casual and informal contexts. With this in mind, there is a gap for something quicker that helps to reinforce basic threats and controls, based upon threats and safeguards that are relevant to general end users. This has led the authors to design, implement and trial a new game, Cyber Defence Dice.

III. CYBER DEFENCE DICE GAME CONCEPT AND DESIGN

In considering how to deliver a game that could be understood and played quickly, it was notable that none of the

existing games had used dice as the focus of their gameplay. Several involve using dice as part of the process, but this is more in the context of making moves, or determining the outcome of an event (e.g. as in Control-Alt-Hack). However, games such as Liar Dice, Poker Dice, and Yahtzee all illustrate how dice themselves can also become the core focus of a game. Poker Dice in particular, with die faces using images rather than numbers, offers a further dimension that often prompts interest from players. As such, it was felt that a dice game could offer both a suitable format for a game and a potential provocation of interest for players (through both the visual appearance of the dice themselves, and by witnessing others playing with them). Meanwhile, keeping a focus on simple, short-form gameplay would aim to ensure that there was a low barrier to entry and engagement.

From this point, resulting design considerations included the identification of a series of suitable threats and controls (including the need for some sort of hierarchy in terms of the severity of threats/attacks) and the need for the gameplay to involve some basic cyber decision making (e.g. what threats beat what controls, and what are the player's options based on the dice rolled?). We selected a series of threats and controls that are generally relevant from both the business and end-user perspectives, as listed in Figure 1. In terms of the threats, it is expected that most end users will be familiar with terms such as malware, hacking, phishing, and would be able to relate to the notion of accidental breaches. By contrast, Denial of Service and - more particularly - Zero Day Attacks are potentially less commonly known, but the accompanying guidance then provides a brief definition of each. Similarly, for the controls, many users would relate to concepts such as backup, updates, secure configuration, awareness, and Internet security (the latter through related tools/packages that they may have installed). Defence in Depth may be less familiar, but the notion is again explained via a brief definition.

Attacker Dice



Malware: Malicious software that may corrupt or steal data, damage systems, and varyingly affect confidentiality, integrity and availability.



Hackers: Attackers gaining (or attempting to gain) unauthorized access to systems and data, often via exploiting technical vulnerabilities.



Accidental Breach: Breaches caused by errors, mistakes and other unintentional actions by legitimate users.



Phishing: Use of social engineering techniques to trick unsuspecting users into sharing sensitive information.



Denial of Service: An attack against availability, preventing systems and data from being accessible by authorized users.



Zero Day Attack: Exploitation of a previously unknown vulnerability. Bypasses all but *Defence in Depth*.

Defender Dice



System and App Updates: Ensuring that your systems are patched against known security vulnerabilities.



User Awareness: Ensuring that users know what to do to identify threats, maintain security, and prevent mistakes.



Backup: Maintaining a safe copy of your system and data files.



Secure Configuration: Ensuring that your protection is set up correctly.



Internet Security: Ensuring protection against a range of online threats and network-based attacks.



Defence in Depth: Attention to security across multiple perspectives, enabling layered and holistic protection.

Fig. 1. Threats and controls represented on the attack and defence dice

The dice are produced in red and blue to reflect the colours commonly associated with the attack and defence roles in cyber security testing [13], with the fact of using coloured dice also being a further potential provocation of interest for players. The pictures on the dice are all original and hand-drawn within the project team, and chosen to reflect imagery that players could then associate with each of the threats. Some (e.g. the Hacker image) are similar to existing depictions of the concepts, whereas others (e.g. Denial of Service) attempt to give a simple visual representation where 'standard' images do not already exist.

The threats and defences are matched against each other as presented by the matrices in Figure 2. It is important to note that from the Attacker perspective, the aim is to test the defences not to bypass or work around them. The top matrix shows how an attacker could respond to controls declared by a defender, while the bottom one shows defences that can respond to prior attacks. For example, if a Defender has opened play with a security posture based on User Awareness, then the Attacker would be able to test this defence using Malware, Accidental Breaches, Phishing, or a Zero Day Attack. Meanwhile, Backup would be an appropriate response if an Attacker has thrown Malware, Hackers or Accidental Breaches, but not for any other attack type.

There is a degree of interpretation in determining what attacks would combat which defences and vice versa. For example, it is shown that all of the controls can provide some protection against malware. However, this applies under particular circumstances, and in reality there would be some forms of malware attack where some controls would *not* apply. For instance, user awareness would be a relevant anti-malware control where the attack vector involves user interaction (e.g. following a link or opening an infected attachment), but would have no impact for malware that

comes in directly via unpatched vulnerabilities. Similarly, there are some cases in which the rules are used to establish the varying 'power' of the dice, but where the real world situation could differ. For example, one could reasonably argue that there is a relationship between Hackers and User Awareness, on the basis that a hacker may use social engineering as a means of gaining access (or obtaining information that contributes towards doing so). However, in the game context, they are not used to combat each other.

For the Attacker (if the Defender played first)

Does this attack test this defence?

	Malware	Phishing	Denial of Service	Insider Threat	Supply Chain	Business Continuity
Download	✓	✓	✗	✗	✗	✓
Network Security	✓	✗	✓	✓	✗	✓
Backup	✓	✓	✓	✗	✗	✓
Settings	✓	✓	✓	✓	✗	✓
Security Awareness	✓	✓	✗	✓	✓	✓
Defence in Depth	✗	✗	✗	✗	✗	✓

For the Defender (if the attacker played first)

Does this defence combat this attack?

	Download	Network Security	Backup	Settings	Security Awareness	Defence in Depth
Malware	✓	✓	✓	✓	✓	✓
Phishing	✓	✗	✓	✓	✓	✓
Denial of Service	✗	✓	✓	✓	✗	✓
Insider Threat	✗	✓	✗	✓	✓	✓
Supply Chain	✗	✗	✗	✗	✓	✓
Business Continuity	✗	✗	✗	✗	✗	✓

Fig. 2. Compatibility of threat and defence types

IV. USING THE DICE

The dice provide a basis for several game variations, each sharing the following common principles:

- each side (individual players or teams) gets a set of five dice – the red set for Attackers, the blue set for Defenders.
- each side has up to three throws but can choose to stop after one or two throws if preferred. *The side throwing in response is then limited to that number of throws.*

There are three suggested games, each with different ways of using the dice and differing gameplay complexity:

- **Match Mode:** The opening player declares an attack or defence for the other player to respond to based on the matching combinations shown in Figure 2. For example, if an Attacker has thrown 3 Phishing dice, then the Defender can counter with 3+ Staff Awareness or Internet Security (or via Defence in Depth, which is a valid defence against all attacks). To win a round players need to throw more defence dice than the corresponding attack (or vice versa). If a matching number of attack/defence dice are thrown (e.g. 3 Malware and 3 Backup), then the round is a draw (no point scored). Attacks and defences must be based on a single die type (e.g. 3 Malware cannot be countered by 2 Backup and 1 Internet Security, even though both dice types are individually valid defences).
 - **Combinations:** Each set of dice has a scale of importance, from lowest to highest (as reflected by the order in which they are presented in Figure 1), and are used in a similar manner to other dice games such as Poker Dice. Players can then throw various dice combinations, in increasing order of value: Two of a kind; Two pairs; Three of a kind; Full range (a full set of five different attacks or defences, with the upper range set beating the lower range – akin to high and low straights in Poker Dice); Combined attack/defence (three of one + two of another, akin to a full house in Poker Dice); Four of a kind; and Five of a kind.
 - **Attack Matcher:** The attacker always throws first, and this variant allows the attack to be based on any combination of dice. The defender can then use up to the same number of throws to obtain a set of dice that fully counters the attack. An attack is countered if, for each attacking die, there is a corresponding defending die that combats it. If the attack is countered, the defender wins, and vice-versa.
- As a worked example, we focus on the 'Match mode' variant of the game, as this was the version that was used as the basis for the series of playtests discussed later. The basic rules of the game in this context are as follows:
- Either side may start the game. Play is then determined by the winner of prior rounds.

- All dice are thrown on the first throw. The player can then choose which to keep or throw again, continuing until they decide to stop or reach a maximum of 3 throws.
- To win, players need to throw more defence dice than the corresponding attack (or vice versa) – e.g. if 2 Malware dice are thrown then Defenders need 3+ homogenous relevant dice to defend.
- If a matching number of attack/defence dice are thrown (e.g. 3 Malware and 3 Backup), then the round is a draw (no point scored).

To show how this works in practice, consider an illustrative round involving the Attacker and Defender players. In this example, the Attacker plays first, meaning that they will set the active threat for the Defender to respond to, and the number of rolls in which they are permitted in order to do so. Figure 3 shows a series of resulting dice rolls from the Attacker. From Roll 1, while DoS is the hardest to beat, the player elects to keep the two Phishing and re-roll the other three. Roll 2 then yields two DoS and an Accidental Breach. The two DoS are better than the two Phishing that were originally kept, and so the player elects to keep these instead and re-roll the other three dice. Roll 3 yields a further DoS and two Zero Day Attacks. The player has the choice of which to declare - the pair of strongest dice or the three of the slightly weaker type. In this instance, they opt for the latter, on the basis that the opposing player needs to throw a higher number of matching dice to win.

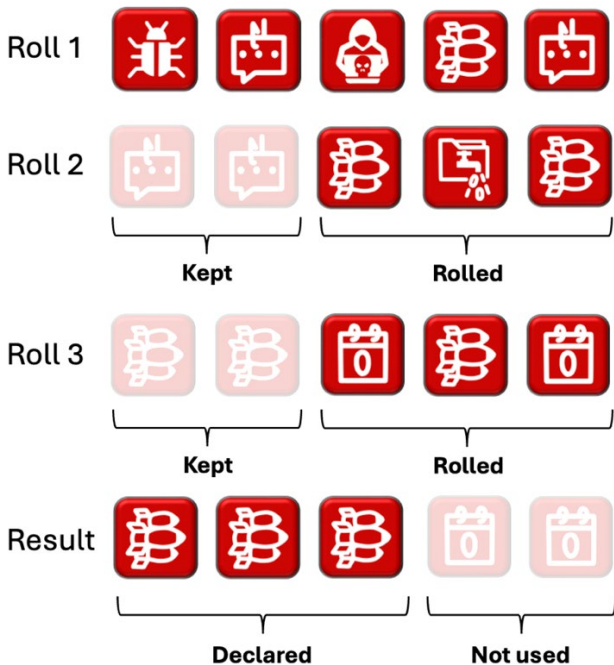


Fig. 3. Example of three rolls from an Attacker

With the Attacker having used the maximum of three rolls, the Defender now has up to three rolls of their own to equal or beat the three DoS dice. This means that they are seeking to roll Internet Security or Defence in Depth controls. Figure 4 shows how the defence plays out. In the first roll the player has thrown nothing of use in combating the DoS threat and so all dice are rolled again. Following Roll 2, the Defender has two pathways – to keep Internet Security or Defence in Depth. While both types could both combat DoS, the rule in Match Mode requires the use of the same defences rather than a mix. The player elects to keep the Internet Security pair, but keeping Defence in Depth would have been equally valid. The third and final roll yields two User Awareness and one Defence in Depth, and so on this occasion the player has failed to mount an effective defence and the Attacker wins.

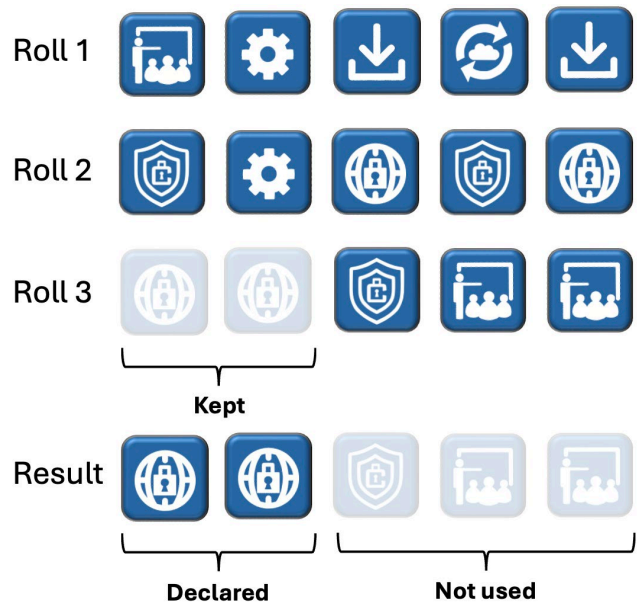


Fig. 4. The Defender's rolls in response to the attack

To give a clear endpoint to the game, it can be played with tokens, as a proxy for the 'budget' of the attacker and defender. Each player places a token at the start of a round, with the winner taking the tokens at the end (or leaving them in the middle and optionally adding to them in the event of a draw). To add a further element to the gameplay, the players can roll one or two standard dice at the start of the game to determine how many tokens they each start with. This can be considered to approximate to another scenario that may occur in real life, with the parties being asymmetric in terms of their capabilities and resources.

V. EVALUATION

The game has been evaluated via a series of hands-on playtests, conducted with a range of different audiences in order to see if the game made sense and delivered value from their differing perspectives on cyber security:

- **Cyber Educators:** Those directly involved in delivering cyber security education to others, and therefore aware of the experience of trying to communicate the concepts to a wider audience.
- **Cyber Professionals:** Those directly working as cyber security professionals in practice, and therefore experienced in working with the threats and safeguards in a real-world context.
- **Cyber Students:** Those learning about cyber security as part of their studies, and therefore generally from a younger age group who will have more recently come into contact with the topic.
- **General Public:** Those for whom cyber security awareness is a relevant consideration even though they are not directly connected with the topic in other ways.
- **IT Professionals:** Those working in IT-based roles, but without a particular specialisation in cybersecurity.
- **Non-Cyber Students:** Those studying at university level, but in topics other than cyber security, again giving access to a younger age group but this time with the expectation of more varied background knowledge and familiarity with the topic.

TABLE I. Playtest Activity Overview

Playtest No. and Location	Date	Participants	Primary audience
1 Las Vegas, USA	29 April 2025	9	Cyber Students
2 Maribor, Slovenia	21 May 2025	10	Cyber Educators
3 Mytilene, Greece	7 July 2025	8	Cyber Educators
4 London, UK	17 July 2025	6	Cyber Professionals
5 Retford, UK	5 August 2025	6	General Public
6 West Bridgford, UK	1 September 2025	6	Non-cyber Students
7 Bucharest, Romania	9 September 2025	10	IT Professionals

A summary of the playtest activities to date and related participation is presented in Table I. These sessions lasted between 45-60 minutes, beginning with a brief introduction to the game and confirming participant consent to participate. This then led into a period of actual gameplay, initially in teams of 3-5 per side and then switching to a series of 1:1 games. There was then an individual participant feedback survey and

a period of follow-on group discussion. The playtest procedure was approved by the School of Computer Science Research Ethics Committee at the University of Nottingham (CS-2024-R44), and all sessions were conducted accordingly. All participants read and signed consent forms before any play began.

The feedback survey gathered some basic demographics, asking about gender, age group, topic background (e.g. area of work or study), familiarity with cybersecurity (self-rated as none, low, moderate, good or advanced) and years of experience (for those participants that were cyber educators or professionals). It then proceeded to collect ratings for a number of factors of the game and their experience of playing it. This was followed by an opportunity to offer free-text comments, prior to engaging in the group discussion. In all tests it was emphasized to the participants that they should respond honestly and that the investigators were interested in receiving genuine feedback.

Space constraints prevent a full discussion of the results, but some key overall results across the 55 participants to date are presented in Figure 5. These charts provide a clear indication of positive feedback, both in relation to the nature and enjoyability of the game, and its potential as an engagement and awareness activity.

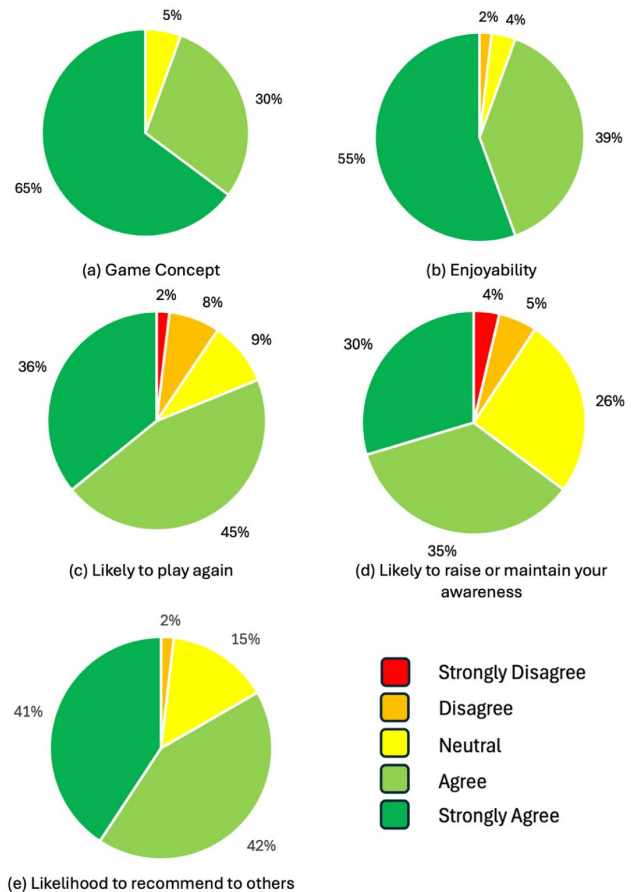


Fig. 5. Ratings collected during the post-play feedback survey

A more granular account, along with thematic analysis for the feedback discussions, will be presented in a future paper, once a further set of playtests have been conducted. However, at this stage there are some further points that can be noted to give context to the overall results:

- Despite the varying nature of the audiences, there was no significant difference between the overall responses from the different playtest groups.
- There were mixed views about whether one-to-one or team-based play was more enjoyable.
- The least positive results are in Figure 5(d), in relation to whether the game would raise or maintain their awareness. However, the results here are somewhat skewed by cyber educators and IT professional groups, who commented that they did not believe it would affect *their own* awareness, but emphasised that they felt it had awareness-raising value for those unfamiliar with cybersecurity concepts (with several participants indicating that they would use the game in this context).



Fig. 6. Examples of written feedback comments

To expand upon the rating-based results, Figure 6 presents some illustrative examples of the written comments that accompanied the ratings, each taken from different participants. In practice far more of the comments fell into the positive category, but for the purpose of balance the table devotes comparable space to the other comments as well. It may be noted that even some of the more critical comments were still provided alongside very positive feedback ratings. Similarly, the feedback in the open discussions that followed the gameplay was dominated by positive comments, with many respondents also suggesting ideas for potential extensions and variations to the game.

VI. DISCUSSION

The results clearly confirmed that the game succeeds as an engagement activity, as players found it enjoyable and many were very much getting into the competitive aspect of the attacks and defences. Moreover, all of the groups had to be instructed to stop the activity so that sessions could proceed to the feedback stage, otherwise they would have happily continued to play. Similarly, these discussions led to some very enthusiastic participation and tended to lengthen the playtest sessions, as participants were keen to offer further ideas and feedback.

This is not to say that the feedback was uniformly positive, and two points of discussion recurred across multiple playtests:

- Participants in the cyber and IT professional sessions both commented that throwing dice is not a good analogy to making cybersecurity decisions (e.g. the observation about "too little agency" from Figure 6). While this is a fair point, insofar as cyber professionals will not select their response to an incident based on chance, the roll of the dice does parallel the notion of having to deal with the unexpected, or to find that your starting point in the response may not be as you would like. Moreover, the incorporation of elements of luck and chance is not unique to this game - it can also be seen to feature in the card-based cyber games if they rely on cards being dealt or drawn from a shuffled deck (and - as a specific example previously mentioned - Control-Alt-Hack involves throwing numbered dice to determine whether players have the required skills to complete tasks within missions).
- Some players observed that they were able to play the game without really understanding the relationships and nuance of the threats and defences - they simply needed to know that Zero Day Attacks and Defence in Depth were the best and to go for these. This is a fair comment and highlights the desirability of preceding play with a briefing about the attacks and defences, or discussing them afterwards (whereas in the playtests the participants were dropped into the situation, and some elected to read the rules in more detail than others). However, given that the same playtests led to extensive discussion about how

the game worked, it still succeeded as a provocation of interest and gave players something to learn from as a result.

The game is, of course, only representing reality to a certain extent, and the parallels break at some point. For example, user awareness will not protect against all forms of malware or accidental breach, and secure configuration is only likely to go some way towards addressing phishing threats. Similarly, a genuine attacker would typically seek to work around the defences and target an aspect that is not defended at all (e.g. if the defence is User Awareness, go for an attack that does not relate to it, such as Denial of Service). However, from a red teaming perspective you are looking to test and compromise the defence that has been put in place, and so in this context the analogy holds.

Ultimately, it is important to remember that Cyber Defence Dice is a *game* and not a *simulation*, but at the same time to recognise that there is still value to be gained within these bounds. The earlier point about dice not being involved in real-life cyber decision-making is of course valid, but the game is still helping to foster some recognition of the threats and safeguards over which decisions need to be made. Similarly, when playing a game such as Monopoly, people do not spend money as they would do in real life, but playing the game still helps to build familiarity with the nature of money and the need to manage it. Likewise, playing with Lego blocks does not qualify someone as a civil engineer, but it can provide some basic appreciation of how to build things that do not fall down. Rather than being an endpoint in itself, the dice game can be viewed as a means of prompting interest and engagement, which in turn provides the basis for a further discussion about the concepts that have been introduced.

VII. CONCLUSIONS

As an awareness-raising activity, the playtests and related feedback suggest that the game succeeds in its aim of providing a provocation of interest, and participants agreed that it would provide a good basis for learning about the basic threats and safeguards. At the same time, there is certainly a limit to what players can gain in terms of building their cyber awareness. For example, it clearly does nothing in terms of training or building capability to handle the threats and apply the safeguards in practice. The findings do, however, support the view that the dice would have a relevant role for initial awareness raising and subsequent reinforcement learning, and the knowledge/awareness levels provided by this game are good relative to the time investment required to understand and play it (i.e. while the cybersecurity coverage is necessarily limited, it is quick to gain).

For those concerned that the scope of the game is too limited, it can also be viewed as a foundation upon which to build further elements of gameplay. As an example, the authors have already established an extension to the Match Mode version of the game, which involves the use of assets that need to be protected by defenders and targeted by

attackers. The assets are represented by physical tokens (thereby giving a further element of tactile and visual interest) and include items such as PC, Personal Data, Website and Email Server (all chosen as things that are likely to be broadly familiar to end-users, and therefore relatable in terms of the need to protect them). While this adds to the resulting length and complexity of the game, it provides a further dimension in linking the experience to the real-world objective of cybersecurity (i.e. a key reason that we want to defend against threats is to protect assets). As such, it offers a means to go further than the basic game for those that want to add further to the learning experience.

ACKNOWLEDGEMENTS

The authors would like to thank all the participants who gave their time to play the game and offer feedback, and the event organisers that offered the opportunity for the playtest sessions to be hosted within their events.

REFERENCES

- [1] Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. 2007. "The design and evaluation of a game that teaches people not to fall for phish", Proceedings of the 3rd symposium on Usable privacy and security (SOUPS '07), pp. 88-99. <https://dl.acm.org/doi/abs/10.1145/1280680.1280692>
- [2] Omotosho, A., Awazie, D., Ayegba, P., Emuoyibofarhe, J. 2021. "A Gamified Technique to Improve Users' Phishing and Typosquatting Awareness". In: Misra, S., Muhammad-Bello, B. (eds) Information and Communication Technology and Applications. ICTA 2020. Communications in Computer and Information Science, vol 1350. Springer, Cham. https://doi.org/10.1007/978-3-030-69143-1_31
- [3] Scholefield, S. and Shepherd, L.A. 2019. "Gamification Techniques for Raising Cyber Security Awareness". In: Moallem, A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2019. Lecture Notes in Computer Science(), vol 11594. Springer, Cham. https://doi.org/10.1007/978-3-030-22351-9_13
- [4] Ophoff, J. and Dietz, F. 2019. "Using Gamification to Improve Information Security Behavior: A Password Strength Experiment". In: Drevin, L., Theocharidou, M. (eds) Information Security Education. Education in Proactive Information Security. WISE 2019. IFIP Advances in Information and Communication Technology, vol 557. Springer, Cham. https://doi.org/10.1007/978-3-030-23451-5_12
- [5] Rikkers, V. and Sarmah, D.K. 2025. "A story-driven gamified education on USB-based attack", *Journal of Computing in Higher Education* 37, 248–272. <https://doi.org/10.1007/s12528-023-09392-z>
- [6] Zhang-Kennedy, L. and Chiasson, S. 2021. "A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education", *ACM Computing Surveys*, 54, 1, 2021, <https://doi.org/10.1145/3427920>.
- [7] Shostack, A. *Tabletop Security Games + Cards*. [Online]. Available: <https://shostack.org/games>.
- [8] Black Hills Information Security. nd. *Backdoors & Breaches: Visual Guide*. https://www.blackhillsinfosec.com/wp-content/uploads/2024/03/BnB_VisualGuide_v2_03052024.pdf
- [9] Denning, T., Lerner, A., Shostack, A. and Kohno, T. 2013. "Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13)*. Association for Computing Machinery, New York, NY, USA, 915–928. <https://doi.org/10.1145/2508859.2516753>
- [10] CIAS. 2024. "Cyber Threat Defender", Center for Infrastructure Assurance & Security, The University of Texas at San Antonio. <https://cdn.getshifter.co/fd026a43ee1b7b095c768a9039a2a236c0a0d590/uploads/2025/07/CTD-Instructions-2025Rulebook.pdf>

- [11] Frey, S., Rashid, A., Anthonymsamy, P., Pinto-Albuquerque, M. and Naqvi, S.A. 2019. "The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game," in *IEEE Transactions on Software Engineering*, vol. 45, no. 5, pp. 521-536.
<https://doi.org/10.1145/3180155.3182549>.
- [12] Hart, S., Margheri, A., Paci, F. and Sassone, V. 2020. "Riskio: A Serious Game for Cyber Security Awareness and Education", *Computers & Security*, Volume 95,101827,
<https://doi.org/10.1016/j.cose.2020.101827>.
- [13] NIST. 2025. "Red Team/Blue Team Approach", Glossary, Computer Security Resource Center, National Institute of Standards and Technology.
https://csrc.nist.gov/glossary/term/red_team_blue_team_approach
(accessed 17/8/25)