

Cybersecurity Awareness: Making a game of it

*Steven Furnell¹, Lucija Šmid², James Todd¹, Xavier Carpent¹ and Simon
Castle-Green¹*

*University of Nottingham, Nottingham, UK
University of Bath, Bath, UK*

contact@cybergameslab.org

Introduction

The use of digital devices and online services is now embedded across many aspects of our personal and working lives, with many individuals and organisations having a high degree of technology and data dependence. At the same time, the existence of cyber threats means that the same users are at risk if they do not have appropriate protection in place. Unfortunately, a key challenge is that technology adoption continually tends to outpace cybersecurity awareness, such that many are readily using the technology without necessarily knowing about the threats or what they should be doing about them.

While there is no shortage of cyber awareness material available if people wish to look for it (e.g. through public-facing cyber awareness websites such as Stay Safe Online in the United States, Get Safe Online in the United Kingdom) this tends to rely upon the audience having the interest and motivation to take the initiative for themselves. Even within organisations, we often find that cyber awareness receives little more than lip-service (e.g. requiring staff to complete periodic ‘online training’ that feels little more than a tick-box exercise) and so fail to provide lessons that are meaningful and/or memorable.

It is therefore desirable to find means of making cybersecurity awareness more engaging and delivering it in ways that may appeal to the target audience. Once such solution is the use of gamification, and related games have been realised in both digital and physical formats. The latter are considered to be particularly interesting, as they provide a basis for supporting in-person cyber awareness activities and building it into more social settings. Against this background, we introduce a new game that has been designed as means of supporting basic cyber awareness.

Gamifying Cybersecurity

There are already several well-recognised and widely referenced games in the cybersecurity space, with examples including Backdoors & Breaches (Black Hills, n.d.), Control-Alt-Hack (Denning et al. 2013), Cyber Threat Defender (CIAS, 2024), Decisions & Disruptions (Frey et al. 2019) and Riskio (Hart et al. 2020). However, of these, only Cyber Threat Defender could be considered to be aimed at the level of the layperson end-user. The others require a level of prior cybersecurity knowledge to play and/or a Game Master with the associated knowledge who can facilitate the game.

In addition, many existing games require some time commitment to play. Cyber Threat Defender is reported to average ~20 minutes per game, while Backdoors & Breaches and Control-Alt-Hack both take up to an hour. Decisions & Disruptions offers the most involved gameplay, with sessions taking up to two hours. For people that may not even be convinced that they want to *play* a cybersecurity game (which could well be the starting point for many users), it is desirable to lower the bar to entry and reduce the level of commitment required to both understand the rules and play the game.

With the above in mind, the authors have designed, developed and evaluated a new tabletop game, Cyber Defence Dice (Furnell et al. 2026). This focuses upon key issues of cyber hygiene, promoting

awareness around what we need to protect, what we are protecting against, and how the protection can be achieved.

The Cyber Defence Dice game

A specific aim in designing the game was to create something that players could understand and play quickly with minimal instruction. A dice-based game was attractive on the basis that it would lend itself to short form play, and also that the dice themselves could help to attract players (with the associated colours and imagery acting as provocation of interest). Additionally, such a dice-based format had not been used at all amongst the existing cybersecurity games.

Having noted that most existing games appeared to target players with some established cybersecurity knowledge, it was considered desirable to aim at a more general audience as a means of promoting cybersecurity awareness. Of particular interest were end users and staff within small organisations, both of whom are relevant audiences that can often lack cyber awareness. From this perspective, there are some fundamental issues and concepts that it was considered relevant for users to be aware of:

- Assets – a mix of physical and digital items of value that need to be protected;
- Threats – events that would potentially cause harm to the assets;
- Defences – safeguards that can provide protection against the threats.

Unlike other dice games, such as Poker Dice (where players share a single set of dice), it was considered that a more appropriate format would be an adversarial game that involved different dice sets for attackers and defenders. The use of Assets then comes into play as something that the two sides are seeking to protect or acquire. The resulting sets of items selected within these categories are presented in Table 1, with the Assets being realised in the form of six individual tokens/chips, while the Threats and Defences are each placed on the faces of six-sided dice. The images for each of the items were hand-drawn by the authors.

Table 1: Assets, Threats and Defences used in Cyber Defence Dice

Assets		Threats		Defences	
	Email Server		Malware		System and App Updates
	Personal Computer		Hackers		User Awareness
	Personal Data		Accidental Breach		Backup
	System Administrator Account		Phishing		Secure Configuration

	Website		Denial of Service		Internet Security
	Wireless Router		Zero Day Attack		Defence in Depth

In selecting the specific Assets, Threats and Defences to be used, there were several considerations to address:

- The items involved needed to be relevant and relatable for different types of audience. They needed to be understandable enough for laypersons, while also remaining realistic and relevant from the perspective of security-aware players.
- There must be some level of variety and/or hierarchy in terms of which attacks will beat which defences (and vice versa), as well as which threats and defences are applicable to attacking or defending particular assets. In this way, players need to understand (and make decisions based upon) how the assets-threats-defences relate to each other – which in turn helps to build the awareness-raising potential of the game. The relationship between threats and defences is shown in Figure 1.
- We wanted to ensure that different perspectives of cybersecurity were represented. For example, cyber threats are not entirely malicious and deliberate in origin, and so Accidental Breaches was specifically included to highlight that not all threats equate to attacks. Similarly, in terms of the defences, it was important to show that cybersecurity is not exclusively about technical safeguards, and so User Awareness was included to reflect the human element (and indeed the aspect that the game itself seeks to support). The same need for variety was also considered in the selection of the assets, where some (e.g. PC and Wireless Router) are physical devices, whereas others (e.g. Admin Account and Personal Data) are digital aspects.

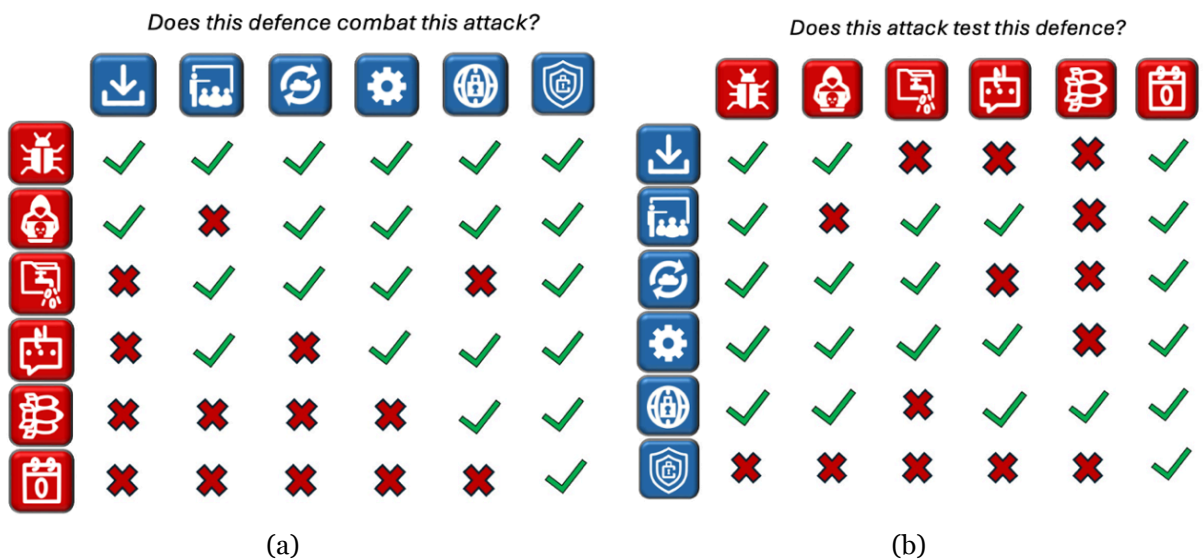


Figure 1: Matrices to show relationship between attacks and defences (a) if Attacker has played first and the Defender needs to check compatible defences; and (b) if the Defenders has played first and the Attacker needs to check compatible attacks.

While most of the threats and defences are typically relatable and often familiar (at least in name) to most users, there are a couple that merit further explanation. Specifically, the Zero Day Attack and Defence in Depth are less likely to be known at the outset. The former was included as a means of having a ‘worst case’ attack that players could then discover/learn about as a result of playing, while the latter helps to offer a further subtle lesson about cyber defence (i.e. the fact that having multiple and/or layered safeguards can provide additional protection).

It is also relevant to briefly explain what was *not* included, where a notable omission on the defensive side would seem to be user authentication. We did not include this because it was felt to be something that players would believe they were doing already (unlike, for example, backing up their data or installing timely updates, which some users may then recognise as gaps). While people may, of course, be doing authentication badly (e.g. with weak passwords etc), this is more difficult to highlight through playing the game. One option could have been to include Multi-Factor Authentication (MFA), but in many scenarios enabling this is not done at the end-user’s discretion, but is instead a decision made and enforced by whoever is offering the service they are using (there are some exceptions, where individuals can elect whether or not to enable additional authentication for personal accounts on other services, but these cases are arguably the exception). Similarly, Passkeys could have been another authentication-related defence option, but this was considered less familiar and (at the time of creating the game at least) not an option that was readily available for users to choose on all services. As such, putting authentication *in general* would have had little awareness-raising value (as most players would consider themselves to be doing it), whereas highlighting specific approaches would have raised awareness of things that players may be less able to act upon.

The basic version of the game is played with just the Threats and Defences, with the Assets then optionally providing a further layer to the gameplay once the basic rules are understood. To this end, and recognising that some scenarios will only ever want to use the quicker and simpler variant, there are two versions of the game – standard and deluxe – as shown in Figure 2. In both cases, all the game elements have been produced in-house via 3D-printing.



Figure 2: Cyber Defence Dice in (a) standard and (b) deluxe formats

A full explanation of various play options can be found at www.cyberdefencedice.com. However, the basic game does not *require* extensive explanation and instruction, and the main rules are summarised as follows:

“Either side may start and has up to 3 throws, but can stop after 1 or 2 if preferred. The responding side is limited to that number of throws. Players choose which dice to keep or throw again. To win a round, throw more defence dice than the corresponding attack (or vice versa). A matching number is considered a draw.”

This text is taken from a reference card provided with the standard game, which also lists the attacks and defences, and the earlier matrices (Figure 1) showing how they inter-relate. In the deluxe version there is a further list for the asset types, plus an additional matrix to show which threats/defences relate to each one.

Discussion and Conclusions

Cyber Defence Dice has succeeded in addressing the original aim of offering an entry-level game that supports cyber awareness, and which presents a low barrier to entry. Depending on the speed with which players make their decisions, several rounds of the standard game can be played in just a few minutes. In contrast, the use of the Assets in the deluxe version has the potential to extend the play considerably, as players need to compete until one side has acquired all of them. As such, the way that the game is used can be adapted to the time available. The gameplay of the Deluxe version offers greater depth and engagement, but the standard version is very well-suited to supporting initial introduction to cybersecurity and works well as an ice-breaker activity or an accompaniment to a wider cyber awareness session.

The game has been evaluated in a series of playtests involving a variety of players (including cybersecurity students, educators and professionals, students from non-cyber disciplines, and the general public) and has proven successful in all contexts. Players have provided positive ratings and feedback in terms of the game concept and its enjoyability. It has also been used in practical contexts, including use in teaching (for computing and non-computing students), public engagement events, and awareness-raising for small businesses.

While playing the game in isolation may have limited value in educating players about the real details of the threats and what they ought to be doing about them, its incorporation into wider cyber awareness activities provides a basis to take things further. As mentioned, it can act as an initial provocation of interest that helps people to more willingly engage in the first place, as well as providing a periodic reminder of past lessons learned (i.e. a basis for reinforcement of learning).

Cyber Defence Dice is one of a series of awareness-raising that the authors have produced. The same set of assets, threats and defences are also utilised in another, arcade-style game called Hacker Whacker (Todd et al. 2026), and the authors plan to expand the usage into other game formats. The result is that players can engage to different extents (depending on the time available and the preferred style of game), but with each activity helping to promote awareness of some core concepts that are of value as a foundation for cybersecurity understanding and good practice.

Acknowledgements

The authors would like to thank all the participants who gave their time to playtest the Cyber Defence Dice game and offer feedback, and the hosts that offered the opportunity for playtest sessions to be run within their premises or events.

References

- Black Hills Information Security. (n.d.). Backdoors & breaches: Visual guide. Retrieved from https://www.blackhillsinfosec.com/wp-content/uploads/2024/03/BnB_VisualGuide_v2_03052024.pdf
- Center for Infrastructure Assurance & Security. (2024). Cyber threat defender. Retrieved from <https://cdn.getshifter.co/fd026a43ee1b7b095c768a9039a2a236coa0d590/uploads/2025/07/CTD-Istructions-2025Rulebook.pdf>
- Denning, T., Lerner, A., Shostack, A., & 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 and communications security (pp. 915–928). <https://doi.org/10.1145/2508859.2516753>

- Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., & Naqvi, S. A. (2019). The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game. *IEEE Transactions on Software Engineering*, 45(5), 521–536. <https://doi.org/10.1145/3180155.3182549>
- Furnell, S., Šmid, L., Todd, J., Carpent, X., & Castle-Green, S. (2026). Roll with it: Awareness raising with cyber defence dice. *Journal of the Colloquium for Information Systems Security Education*, 13(1).
- Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95, 101827. <https://doi.org/10.1016/j.cose.2020.101827>
- Todd, J., Furnell, S., Castle-Green, S., Šmid, L., & Carpent, X. (2026). Hacker whacker: An interactive game for cybersecurity education. In *Proceedings of HCI-CPT 2026* (forthcoming).