CYBER DEFENCE DICE™

An Awareness Raising Game of Attack and Defence

WWW.CYBERDEFENCEDICE.COM

Testing a defence

(i.e. defender played first)

Defending against an attack

(i.e. attacker played first)

The Dice

The dice are based on common forms of cyber threat and the defences that can help to protect against them. These are listed and described in the tables below.

Attacker Dice

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

Hackers: Attackers gaining (or attempting to gain) unauthorised 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 authorised 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.

General Rules

Each side (individual players or teams) gets a set of five dice – the **red** set for Attackers, the **blue** set for Defenders.

Each round can have up to three throws per side, but the side throwing first can choose to stop after one or two throws if preferred. *The side throwing second is limited to the number of throws taken by the first side.*

At the end of a round, sides win, lose or draw based on the dice thrown.

See the individual game types for further rules in each variant.

Game Types

Game 1 – Match Mode

[2 Players / 2 Teams]

The aim is to match against an attack or defence thrown by the opening side, by responding with a compatible defence or attack.

Attackers or Defenders may start the game, and play is then determined by the winner of prior rounds.

Players choose which dice to keep or throw again, and may change their mind on which to keep from one throw to the next.

After their chosen number of throws (to a maximum of 3), the opening side declares what their resulting attack or defence is.

All dice in a declared attack or defence must be of the *same* type (e.g. an attack cannot be a mix of Malware and Hackers – one or the other must be declared).

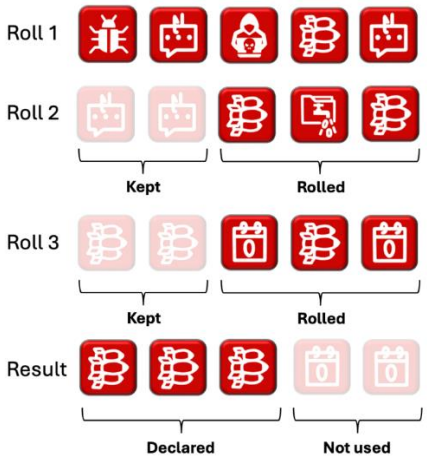
To win a round, players need to throw more defence dice than the corresponding attack (or vice versa). A matching number is considered a draw.

Combined Attacks or Defences can be used to defeat any type of declared attack/defence:

- a *Combined Attack* is a set of Malware, Hackers, Accidental Breach, Phishing, and Denial of Service.
- a *Combined Defence* is a set of Updates, User Awareness, Backup, Secure Configuration, and Internet Security.

Match Mode Example

The example below illustrates a round of a Match Mode game. In this instance the attacker is playing first and takes three rolls. The defending player then responds to the declared attack.

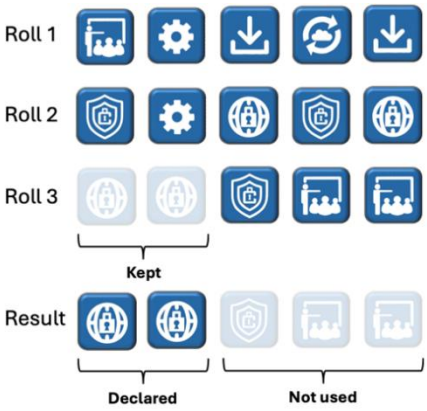


From Roll 1, the player elects to keep the two Phishing dice and re-roll the other three.

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 keeps 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. They opt for the latter, on the basis that the opposing player needs throw a higher number of matching dice to win.

The Defender now has up to three rolls to equal or beat the three DoS dice, so they are seeking to roll Internet Security or Defence in Depth controls.



In Roll 1 they throw nothing of use and so all dice are rolled again.

From Roll 2, they have two pathways – to keep Internet Security or Defence in Depth. Both types combat DoS, but Match Mode requires the use of the *same* defences rather than a mix. The player keeps the Internet Security pair, but keeping Defence in Depth would have been equally valid.

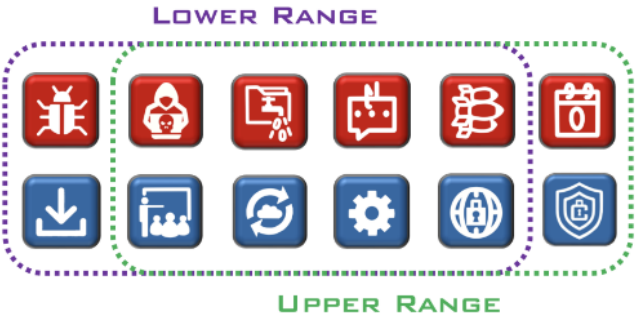
Roll 3 yields two User Awareness and one Defence in Depth, and so the player has failed to mount an effective defence and the Attacker wins.

Game Types

Game 2 – Combinations

[2+ Players]

Each set of dice has a scale of importance (from lowest to highest) and are used in a similar manner to other dice games such as Poker Dice:



Valid dice combinations, in increasing order of value, are then:

- Two of a kind
- Two pairs
- Three of a kind
- Full range attack or defence (a full set of five different attacks or defences, with the upper range set beating the lower range – see the image above for the ranges)
- Combined attack or defence (three of one + two of another)
- Four of a kind
- Five of a kind

For 2 players:

- Players can use a single type of dice (e.g. each using the Attacker dice and seeing who gets the strongest attack), or both types (e.g. an opening player starting with an attack and a responding player countering with a defence, or vice versa).

For 3+ players:

- Choose a single type of dice (i.e. Attack or Defence), and each player takes a turn to throw the best combination.

Game Types

Game 3 – Attack Matcher

[2 Players]

The attacker always throws first, and up to 3 times.

The defender can then take up to the same attempts to throw a set of dice that counter the attack.

An attack is countered if, for each attacking die, there is a corresponding defending die that beats it (see the image below for the defences that counter each attack).

Each defending die can only be used to counter one attacking die.

If the attack is countered, the defender wins; and vice-versa!

Using Budgets

To give a clear endpoint to the game, it can be played with tokens/counters, which then represent the 'budget' of the attacker and defender.

Each side 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 approximates to real life, where attackers and defenders may be unequal in terms of their capabilities and resources.

Parallels to Reality

[For those that want to know]

Cyber Defence Dice is a *game* and not a *simulation*, and so there are some aspects that do not directly reflect cyber security in real life. For a start, there is typically no dice throwing involved ☺

There are, however, some areas where parallels to real life are possible:

- All of the cyber threats and defences are things that exist in the real world, and the mappings between them (i.e. what beats what) are genuine.
- Players need to understand the cyber threats and safeguards, and make decisions about what defences are suitable against an attack (or vice versa).
- If the Attacker throws first, they are potentially catching the victim unawares, and the Defenders are applying security in a responsive manner.
- If the Defender throws first, it's like they're deciding what to invest in and finding out if they chose correctly. For the attacker it's like they've done reconnaissance and know what to attack.
- When attacking a pre-declared defence, it is analogous to the cyber security practice of Penetration Testing, where an organisation will sanction a test of its defences and the 'attacker' is an authorised security tester.
- The winner of a round starts the next round – so a successful attack has the chance to escalate, and successful defence has a chance to maintain more effective protection.
- When playing using budgets, this reflects the real-world scenario that may occur with one side having more resources than the other.

Using Assets

[Deluxe Version Only]

Introduction

Assets are an expansion of the Match Mode version of the game, adding a further dimension to the gameplay as players are now competing for things to attack and defend.

The game offers six types of assets, all representing things that attackers may wish to exploit, and that their owners will want to protect.

PC

Personal Data

Website

Email Server

Administrator Account

Wireless Router

Distributing the Assets

At the start of the game, Assets can be distributed in different ways:

- Split equally, such that side starts with three Assets. Play continues until one side has acquired all six.
- Play starts with all six Assets in the middle. Play continues until one side has acquired all six.
- Play starts with all six Assets held by the Defender. The Attacker has *N* rounds in which to acquire all six (where the players agree *N,* but 15 is a suggested value). Note that in this version of the game, the Attacker always starts and chooses the Asset they wish to target.

Gameplay with Assets

Each round begins by nominating an Asset to play for. This can be done by:

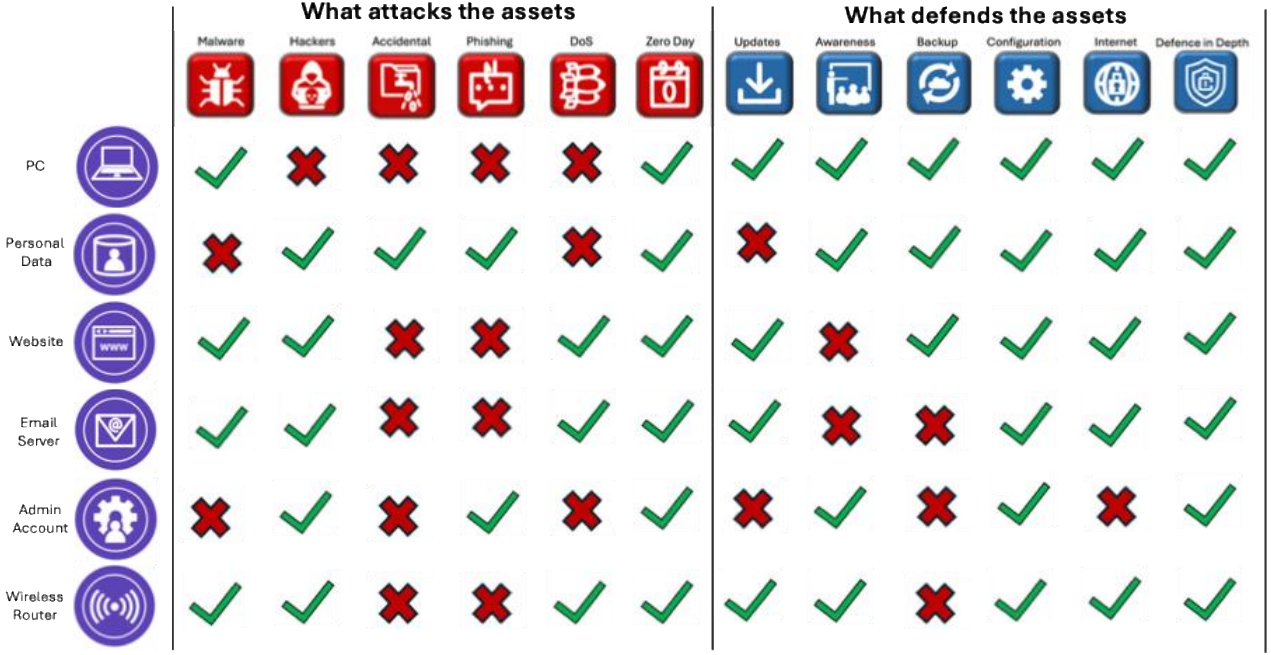
- direct choice (if Assets are face up)
- blind choice (with Assets face down)
- rolling the Assets die.

The starting side attempts to throw an Attack or Defence appropriate to that Asset (see Assets matrix below)

If a valid combination is thrown, the responding side uses the standard Match Mode attack/defence matrix. If a valid combination is not thrown, play switches to the other side.

To *win* the Asset the responding side needs to beat the opening side's throw.

If the opening side wins the Asset, they continue to lead the next round. If not, the Asset stays where it is and play switches to the other side to start the next round


What attacks the assets
What defends the assets
Malware
Hackers
Accidental
Phishing
DoS
Zero Day
Updates
Awareness
Backup
Configuration
Internet
Defence in Depth
PC
Personal Data
Website
Email Server
Admin Account
Wireless Router