DEFENCE CYBER DICE

- Either side may start the game. Play is then determined by the winner of prior rounds.
- The starting player has up to three throws but can stop after one or two if preferred. *The second player is then limited to that number of throws.*
- All dice are thrown on the first throw. Players can then choose which to keep or throw again, continuing until they decide to stop or reach the maximum 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+ of other 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).

Attacker Dice

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

Malware
Malicious software that may corrupt or steal data, damage systems, and varyingly compromise confidentiality, integrity and availability. Includes ransomware, spyware and viruses.

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 or access credentials.

Denial of Service Attack
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 *Holistic Security*

Defender Dice

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

Staff Awareness and Training
Ensuring that users know what to do to identify threats, maintain security, and prevent mistakes.
Combats: *Accidents, Malware* and *Phishing*

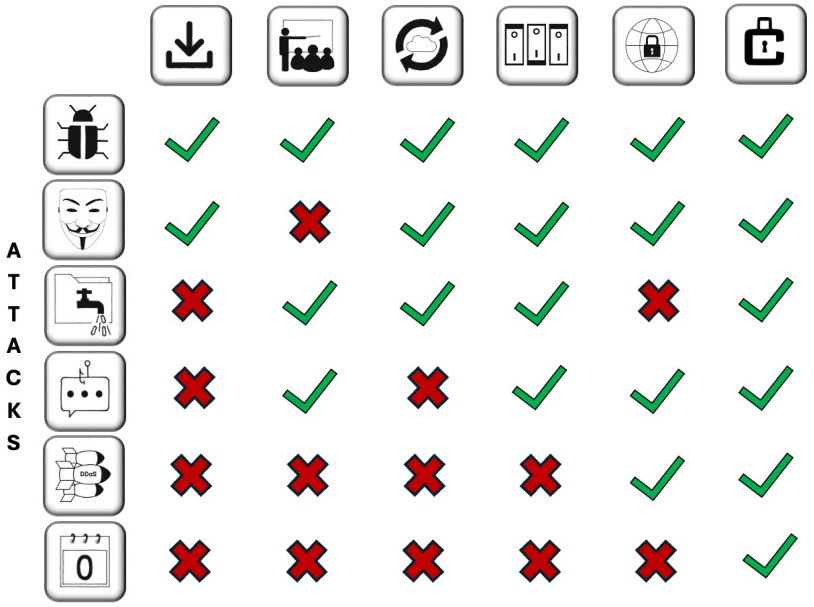
Backup
Ensuring a safe copy of your system and data files.
Combats: *Accidents, Malware* and *Hackers*

Secure Configuration
Ensuring that your protection is set up correctly.
Combats: *Accidents, Malware, Hackers* and *Phishing*

Internet Security
Ensuring that users know what to do to identify threats, maintain security, and prevent mistakes.
Combats: *DoS, Malware, Hackers* and *Phishing*

Holistic Cybersecurity
Attention to security across multiple perspectives, enabling holistic protection and defence-in-depth.
Combats: *All threats, including Zero Day Attacks*

Does it defend against the attack?



Zero Day Attacks can be defeated by throwing a full set of individual controls (i.e. *Backup, Configuration, Updates, Internet Security, and Staff Awareness*)

Holistic Cyber Security can be attacked by a throwing a full set of non-Zero Day attacks (i.e. *Malware, Hackers, Phishing, Accidental Breach, and DoS*)

© Steven Furnell[1], Lucija Šmid[2], James Todd[1] and Xavier Carpent[1]
[1]School of Computer Science, University of Nottingham
[2]School of Management, University of Bath