Cyber Security Awareness Via Gamification: Lessons From Decisions & Disruptions

Benjamin Shreeve
University of Bristol, UK
ben.shreeve@bristol.ac.uk

Joseph Hallett
University of Bristol, UK
joseph.hallett@bristol.ac.uk

Richard Atkins
Metropolitan Police Service
richard.M.Atkins@met.police.uk

Awais Rashid
University of Bristol, UK
awais.rashid@bristol.ac.uk

Abstract
Games are a powerful and usable tool to help raise awareness of cyber security. We report on lessons learned from developing Decisions & Disruptions: a game developed as a research tool, but which has gone on to have multiple versions, and be used by a UK national public organisation as a tool to raise awareness of cyber security nationwide. To date Decisions & Disruptions has been played by more than 2,000 participants, and with more than 200 different organisations. We report on the challenges we faced and the lessons we learned developing and updating different versions of the game; and some of the security perceptions users have when playing.

Author Keywords
games; education; lessons learned

ACM Classification Keywords
J.4 [Computer Applications]: Social and Behavioural Sciences; K.3.m [Computers and Education]: Miscellaneous; K.6.1 [Computers and Education]: Training; D.4.6 [Operating Systems (C)]: Security and Protection

Introduction
Decisions & Disruptions (D-D) is a game designed to explore people's perception of security and their security decision decision making processes. The game started as a

Investments available

Cyber Security Basics
Plant Firewall $30,000
Office Firewall $30,000
Antivirus $30,000
Security Training $30,000

Advanced Cyber Security
Plant Network Monitoring $50,000
Office Network Monitoring $50,000

Physical Security
Plant CCTV $50,000
Office CCTV $50,000

Intelligence Gathering
Threat Assessment $20,000
Asset Audit $30,000

Cards unlocked by Asset Audit
PC Upgrade $30,000
Server Upgrade $30,000
Controller Upgrade $30,000
Database Encryption $20,000
PC Encryption $20,000

research tool but has evolved into something run throughout the UK by a national public organisation responsible for cyber security awareness, and played with thousands of people and hundreds of companies.

Playing the game with a large number of people has reenforced the need to raise public and corporate awareness of cyber security as current security perspectives can be wrong, dangerous or misleading. Some players believe that good security will increase the likelihood of an attack:

> *A:* "... let's say you've got 10 companies and one's got a firewall, you've gotta find which firewall it is, particularly a good firewall, then that's the company they're gonna target..."
>
> *B:* "There could be something good in there."

Others suggest that security has become routine with defenses being deployed by people without understanding their context:

> "It does feel that you'd need firewalls because we always have firewalls."

Many cyber security games have been developed to help improve peoples' security awareness [2, 5, 4, 7, 3, 1, 6]. In this poster we reflect on some of the lessons we've learnt while developing D-D, and how we can educate users about security through games more effectively.

D-D for Research

D-D was originally developed by Frey et al. [3] to explore cyber security decision making amongst different demographic subgroups such as computer scientists, cyber security experts and managers within Academia and Industry.

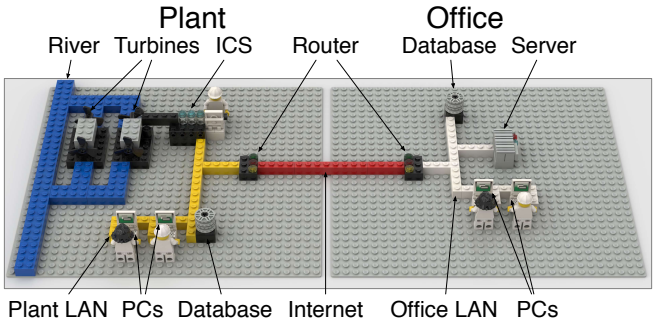
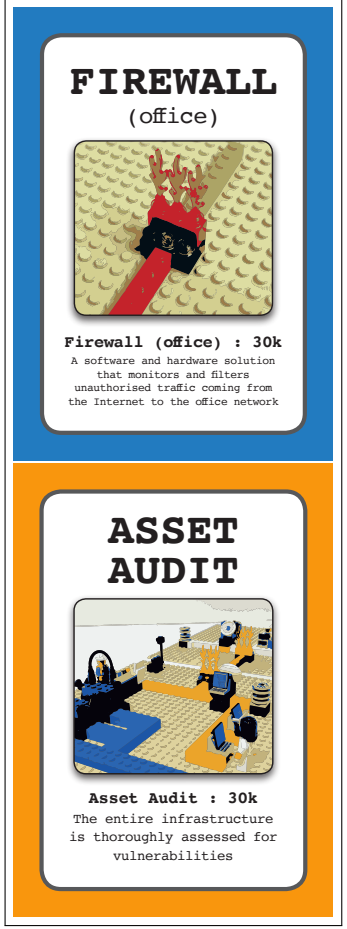


Figure 1: Starting layout for D-D (without any cyber security in place)

During the game, D-D challenges participants to work together as security advisors for a fictional hydro-electrical company. The company operates on two separate sites: A plant site where the company generates electricity, and an office which is located elsewhere. Teams are presented with a physical representation of the organisation and its infrastructure in built in LEGO® (see Figure 1).

Teams are told that this hydro-electric company currently has no cyber security specific defences in place and that they have been asked to help them identify which defences they should invest in and in what order. Teams then have to identify investments from a range available (see sidebar) over four rounds. They are given a budget of $100,000 (game $) to spend in each round (they are allowed to roll over any unspent money between rounds). At the end of each round teams are told about attacks that the organisation has suffered as a result of their investments. There are 30 attacks varying from low-level attacks through to the destruction of the plant. Attackers include Script Kiddies, Organised Crime Groups and Nation States.

Example Investment Cards



This first version of D-D was used to gather research data for Frey et al.'s paper [3] with 43 participants, along with data from a further 137 participants in other sessions. Feedback from these sessions suggested two key changes be made to improve D-D:

Don't be subtle. Attacks suffered needed to be more extreme. Inexperienced participants had a tendency to overlook the potential consequences of the more subtle attacks in the original version. More acute attacks were necessary for teams to appreciate the consequences of their choices. **Take-away:** *Make the players understand that their decisions have consequences, otherwise they won't learn the lessons you're trying to teach.*

Hit them where it hurts. Financial implications were needed. Organisations consistently asked what the potential financial consequences of attacks and decisions might be. **Take-away:** *Consequences have to be delivered to the players in a format they understand—if they don't understand how bad an attack is, they won't learn why they should care.*

D-D for Business

The second iteration of D-D was developed in conjunction with the national public organisation which specialised in raising cyber security awareness and sought to address these shortcomings. The adaptation of D-D retains many of the core aspects of the original game. Teams are still working to help improve things for a hydro-electric organisation which has the same infrastructure. Teams also have the same $100,000 budget to spend across four rounds and on the same potential investments. However, teams encounter a different set of attacks in response to their investments, these attacks tend to have more tangible consequences. Many of these attacks detail the amount which a team may lose as a result of the attack. These losses are used as an additional game mechanism when playing with multiple teams simultaneously; each team adds up their total losses from attacks and the team which loses the least is considered the *winner*.

Everyone has a favourite. While playing the game we noticed that some participants were more interested in the business aspects of the game and disengaged with more technical parts, and that for other players the opposite was true. **Take-away:** *Not everyone cares about the same thing. If you make your game too focused on one thing you risk disengaging those interested in other aspects.*

Everyone has an angle. When playing the game we found that teams with differing levels of seniority and experience gained the most. Contrasting perspectives helped everyone learn from each other and identify new security angles. **Take-away:** *It is important that everyone in an organisation gets a chance to play—not just the technical teams and new recruits. Mix it up!*

Hit me baby one more time! Having played the game once players would wonder what would have happened if they did things differently. D-D has a relatively static script and no randomised elements: players didn't get as much out of a second playthrough as they'd have hoped. **Take-away:** *Cyber security awareness cannot be developed through a single play through, therefore the game needs to be developed so that participants are able to play it through multiple times, encountering different scenarios each time.*

People have jobs to do. Developing a game which will be used by organisations means working within their constraints. For the most part this means developing a game that can be played over a short period. When D-D was played for research, games could last for up to 2 hours, but once we started to play it with organisations this dropped to 1 hour in most cases. This is a reflection of the time constraints placed by organisations on training time.

D-D for GDPR

In 2016 the General Data Protection Regulation (GDPR) came into effect in Europe. This legislation created new rules for how companies had to manage and protect the data of European citizens—and introduced heavy fines for any company that failed to protect the data.

You have to stay relevant. As GDPR came into force we noticed that players would ask what it might mean for them in terms of penalties and consequences they may suffer. D-D was originally developed before the introduction of the GDPR, but in order to stay relevant, we updated seven in game events. These included penalising teams which failed to protect sensitive customer data, and ensuring that teams were told when prior investments protected them from breaches which would otherwise have been of interest to the Information Commissioners Office (legislative enforcer). **Take-away:** *People are aware of big changes in the operating landscape—you need to respond to these otherwise you risk becoming irrelevant.*

Initial findings

Participants demonstrated a number of common cyber security awareness characteristics, we summarise below.

The Windows 95 Effect. Teams believe Firewalls and Antivirus to be key to cyber security, but they rarely explain why. We would posit that this is because Firewalls and Antivirus have been the core basis of 'security' on PCs for the last 30 years.

The Mr Robot Effect. Teams place a far greater emphasis on investing in new defences against uncertain (and inherently unknowable) threat actors rather than investing in upgrades for known existing vulnerabilities.

The Butterfly Effect. Teams often consider what knock-on effect their decisions might have. This appears to be particularly common where teams lack the technical experience in order to make as informed a choice as possible.

Conclusion

D-D was established as a research tool but has since been developed into a dedicated tool for raising cyber security awareness in organisations. This second iteration developed by a national public organisation in the UK has now been extensively used. The data gathered to date has started to provide some insight into cyber security awareness. Furthermore, our experience running D-D enables us to provide some insight for those looking to develop awareness games in the future. Future work will look at *why* people play the way they do and continue to evolve the game to help educate people about cyber security decision making.

REFERENCES

1. Kevin Bock, George Hughey, and Dave Levin. 2018. King of the Hill: A Novel Cybersecurity Competition for Teaching Penetration Testing. In *2018 USENIX Workshop on Advances in Security Education (ASE 18)*. USENIX Association, Baltimore, MD, 9. https://www.usenix.org/conference/ase18/presentation/bock

2. Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. 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)*. ACM, New York, NY, USA, 915–928. DOI: http://dx.doi.org/10.1145/2508859.2516753

3. Sylvain Frey, Awais Rashid, Pauline Anthonysamy, Maria Pinto-Albuquerque, and Syed Asad Naqvi. 2017. The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. *IEEE Transactions on Software Engineering* (2017), 16. DOI: http://dx.doi.org/10.1109/TSE.2017.2782813

4. Mark Gondree and Zachary NJ Peterson. 2013. Valuing security by getting [d0x3d!]: Experiences with a network security board game. In *Presented as part of the 6th Workshop on Cyber Security Experimentation and Test*. USENIX, Washington, DC, USA, 8.

5. Mark Gondree, Zachary NJ Peterson, and Tamara Denning. 2013. Security through play. *IEEE Security Privacy* 11, 3 (May 2013), 64–67. DOI: http://dx.doi.org/10.1109/MSP.2013.69

6. John R. Morelock and Zachary Peterson. 2018. Authenticity, Ethicality, and Motivation: A Formal Evaluation of a 10-week Computer Security Alternate Reality Game for CS Undergraduates. In *2018 USENIX Workshop on Advances in Security Education (ASE 18)*. USENIX Association, Baltimore, MD, 11. https://www.usenix.org/conference/ase18/presentation/morelock

7. Jan Vykopal and Miloš Barták. 2016. On the design of security games: From frustrating to engaging learning. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)*. USENIX Association, Austin, TX.