

Title:

Securing the Future: exploring cybersecurity behaviours and technology adoption in small businesses and start-ups through a game-based simulation

Authors:

Oishee Kundu, Joanna Syrda, Johnny Swierczynski, Tobias Weickert, Adam Joinson

Affiliation:

School of Management, University of Bath

Corresponding author:

Oishee Kundu ok463@bath.ac.uk

Title:

Securing the Future: exploring cybersecurity behaviours and technology adoption in small businesses and start-ups through a game-based simulation

Abstract:

Small businesses and start-ups often lack dedicated resources for cybersecurity, and there is a growing interest among practitioners and policymakers about the factors affecting digital security behaviours and the enablers and barriers to new secure technology adoption. Additionally, the expanding digital world is making cybersecurity a general rather than a specialist skill, and there is a growing need for multi-disciplinary and accessible training resources. Games offer a solution to both these requirements, serving as research tools and teaching aids, facilitating the exploration of perceptions, beliefs, and biases about digital security while providing an engaging platform for learning. This paper introduces a game-based simulation to investigate investment behaviours in start-ups and their technology adoption, while also evaluating the game's efficacy in increasing interest in cybersecurity among non-technical audiences.

(127 of 150 words)

Track: e-Business and Information Systems Management

Word count: 7286 (excluding references)

1. Introduction

In an expanding digital world, characterised by the growing presence of digital devices and the Internet of Things, digital security or cybersecurity has become increasingly important. Cyber-attacks like data breaches and ransomware attacks pose significant risks to both individuals and businesses and disruptions in digital services can have significant impacts on the economy and society (Huang *et al.*, 2023). The UK Cyber security breaches survey 2024 reports that 58% of small businesses identified cyber-attacks in a 12-month period, and 29% were victims of cybercrime (DSIT and Home Office, 2024). Small businesses and start-ups are unlikely to have a dedicated cybersecurity budget or specialised IT and digital security teams, and are therefore particularly in danger of falling into the dark side of a ‘security divide’ in the digital world (Heidt, Gerlach and Buxmann, 2019).

There are two problems when we consider the situation of small businesses from a digital security and information systems management perspective. Firstly, there is limited knowledge about cybersecurity decision-making or the psychology of digital security adoption. Most cybersecurity investment models do not take the opportunity cost of product development, marketing, and other business operational needs into account. For many businesses, cybersecurity may be a credence good, i.e., a good or service whose qualities are not perfectly identified even after adoption or use. This makes it difficult to assign value to digital security in business optimisation, and start-ups may struggle to allocate limited resources to digital security. Existing research suggests that imperfect information about cyber defence measures and the interdependencies between firms often cause businesses to make sub-optimal cybersecurity investment decisions (Ezhei and Tork Ladani, 2020; Fedele and Roner, 2022). However, we know relatively little about the perceptions, biases, and barriers which affect cybersecurity investment decisions of entrepreneurs and start-ups.

Secondly, unlike large organisations which can have technology specialists, a small business or start-up is characterised by individuals playing multiple roles in the organisation. Information security skills then become a general requirement rather than a specialist role (Posey *et al.*, 2013; Burns, Posey and Roberts, 2021). Innovative pedagogical tools like games are positioned as more accessible learning resources to overcome technical knowledge barriers and have been developed in the cybersecurity domain as well (Connolly *et al.*, 2012; Denning *et al.*, 2013; Allal-Chérif, Bidan and Makhoulouf, 2016). Educational games are often found to produce greater engagement and better learning outcomes and can be interesting to people who might otherwise be intimidated by technical terms and other knowledge demands (Anvik, Cote and Riehl, 2019; Younis and Alghamdi, 2021). However, there are relatively few games that address cybersecurity in the wider context of business management where an organisation’s objective is revenue generation and increasing market share, rather than cybersecurity.

This paper addresses the two problems by using a game to better understand decision-making on digital security in the context of small businesses and digital start-ups and evaluates the role of the game in raising cybersecurity awareness among non-technical audiences, particularly those in business and management domains. There is a growing interest in using games for research and learning. Games provide non-hierarchical, interactive, and immersive environments which help players externalise or express their inherent knowledge and beliefs (Allal-Chérif, Bidan and Makhoulouf, 2016; Illingworth and Wake, 2021). Thus, it can be a powerful research tool to draw out perceptions, beliefs, and biases about digital security and understand resistance or barriers to technology adoption. At the same time, games are also an effective teaching tool – Connolly *et al.* (2012) point out that “modern theories of effective learning suggest that learning is most effective when it is active, experiential, situated, problem-based, and provides immediate feedback”, and a game usually meets all these criteria.

We anticipate that our work will be of interest to the research community on e-Business and information systems management as our game combines business management and cybersecurity. We focus on the experience of start-ups and SMEs and the game allows us to observe cybersecurity technology adoption decisions of organisations facing resource constraints. Our observations will therefore also contribute knowledge for policymaking to support small businesses in the digital world, an explicit concern in UK policy (BEIS *et al.*, 2022; DCMS, 2022).

2. Literature review

The pervasive integration of ICT technologies within businesses, particularly accelerated by the Covid-19 pandemic (Wendt *et al.*, 2022), underscores the importance of cybersecurity. As businesses increasingly lean on digital infrastructure, the importance of cybersecurity also increases because a disruption in digital services or data breaches can have significant ramifications on cashflows, business operations, as well as reputation (Makridis, 2021). Small businesses and start-ups are particularly constrained in their ability to invest in cybersecurity due to resource constraints. However, the adoption of digital technologies requires an investment in digital security as well.

2.1 Digital transitions and cybersecurity adoption

What are the drivers for investing in cybersecurity? Traditionally, such questions have been studied through the lens of technology acceptance models which first originated in the 1960s to understand the factors that contribute to successful (or unsuccessful) adoption of a technology, specifically how attitudes connect to the intention to use a new technology. Over 20 such models exist - some explaining adoption in organisational contexts, some in the individual context, and some theories have originated from different strands of research in isolation i.e., sociology or psychology (Taherdoost, 2018). As technology has continued to advance in recent decades, new models have been developed to better explain human behaviour in these novel contexts (Yadegari, Mohammadi and Masoumi, 2022). We review three key models below to illustrate the contextual space for decision-making faced by a new digital business with respect to cybersecurity.

2.1.1 Technology Acceptance Model (TAM)

The technology acceptance model (TAM) (Davis, 1989) originates in two psychological theories: the Theory of Reasoned Action and Theory of Planned Behaviour developed by Fishbein and Ajzen (1975) and Ajzen (1991) respectively. These theories explain the relationship between attitudes and behaviour stipulating that one's intention to perform a behaviour is the best indicator of whether that behaviour will be performed. The original model stipulates that 'perceived ease of use' and 'perceived usefulness' attitudes predict intention of use, which in turn influences actual use behaviour.

TAM was later extended by Venkatesh and Davis (2000) to include several new external factors relating to social influence (e.g., subjective norms) and cognitive instrumental processes (e.g., job relevance). The model was further updated by Venkatesh and Bala (2008) to include additional explanatory variables relating to individual differences and people's beliefs about the technology. However, TAM does not take into consideration other important variables such as cost (Lunceford, 2009) which can play a critical role in decision-making for small e-businesses and start-ups.

2.1.2 Unified Theory of Acceptance and Use of Technology (UTAUT)

The Unified Theory of Acceptance and Use of Technology (UTAUT), developed by Venkatesh *et al.* (2003), emerged from the need for a single theoretical model that could be used to explain technology acceptance with sufficient predictive power. UTAUT proposes four variables which predict behavioural intention, which in turn influences actual use or adoption. The variables 'performance expectancy' and 'effort expectancy' are well aligned with the two predictors explained above under TAM (Davis, 1989; Venkatesh *et al.*, 2003). The third predictor, 'social influence' is defined as "the degree to which an individual perceives that important others believe he or she should use the new system" (Venkatesh *et al.*, 2003). Lastly, 'facilitating conditions' is defined as "the degree to which an individual believes that organisational and technical infrastructure exist to support the use of the system" (Venkatesh *et al.*, 2003). It is also the only predictor that has a direct effect on actual use and is not mediated through intention. Facilitating conditions like regulation and standard-setting, along with subsidies and technical support can play a critical role in technology adoption and prompt firms to invest in cybersecurity measures (Tomlinson, Parkin and Shaikh, 2022).

2.1.3 Diffusion of Innovation theory

Diffusion of Innovation theory developed by Rogers (1962) outlines how new technologies are adopted from a societal perspective rather than an individual or organisational perspective. The theory suggests five elements which influence technology adoption (Table 1), making reference to the perception of the technology itself (is it innovative?) as well as the characteristics of consumer and user groups who adopt innovation (Figure 1).

Table 1 Five key elements of Diffusion of Innovation theory outlined in Rogers (1962)

The Innovation	Firstly, the new technology must be viewed as innovative, meaning ‘new’, before it can be adopted.
Adopters	The theory proposes five categories of consumer groups defined by the point in time when they adopt the innovation (Figure 1). Each group of consumers possesses differing demographic and psychographic traits that influence their adoption decision-making i.e., the costs and benefits that they consider when adopting and at what point in time the consumer makes their decision.
Communication channels	Communication channels refers to the idea that innovation diffusion occurs within a social context therefore channels refer to the flow of information between people which is important for adoption of an innovation to occur.
Time	Innovation adoption on a societal scale cannot occur overnight hence the time element refers to how different consumers make adoption decisions in different time periods and lengths of time.
Social system	Social system refers to both the external (e.g., the media) and internal factors (e.g., position in social group) that influence the decision to adopt a technology.

According to Diffusion of Innovation theory, when individuals consider adopting a new technology their decision-making is influenced by several factors. First, they assess the innovation’s relative advantage compared to available alternatives. Second, they evaluate its compatibility with their values, norms, and personal needs. The third factor, complexity, is similar to the concept of perceived ease of use described by Davis (1989) meaning potential users will evaluate how difficult or easy a technology is to use. Additionally, trialability will determine adoption, as people often prefer to test an innovation before fully adopting it. Moreover, observability plays a role, as individuals need to witness the benefits of a particular technology in order to adopt it themselves. Finally, the concept of “reinvention” refers to the user's ability to modify the technology over time, learning from the experiences of previous adopters (Hays, 1996; Rogers, 2003; Greenhalgh et al., 2004).

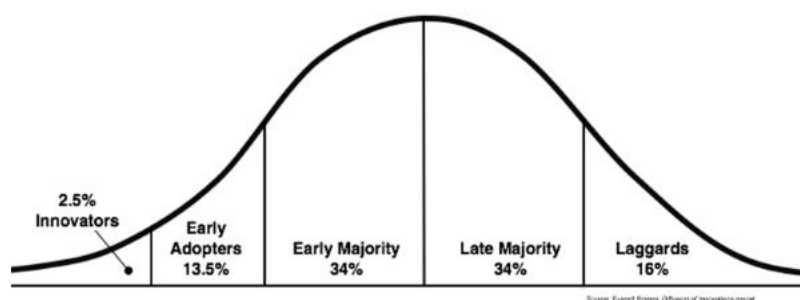


Figure 1 Diffusion of Innovation Model (Rogers, 1962)

Source: <http://blog.leanmonitor.com/early-adopters-allies-launching-product/>

The Diffusion of Innovation theory has been applied to understand firm adoption of digital technologies like cloud computing (Oliveira, Thomas and Espadanal, 2014) and cybersecurity (Hasani et al., 2023), as it takes into account both the innovation and the adopter, considering issues of relative advantage, compatibility, and complexity.

2.2 Economics of cybersecurity

Technology adoption models draw on psychological constructs like perceived usefulness, ease of use, and social influence to explain why firms choose a particular technology. However, they are criticised

for not including the harsh reality of cost or affordability (Lunceford, 2009), which makes it important for us to include knowledge from economics to build a more comprehensive understanding of motivations for cybersecurity investment at the firm-level. Economic theories provide valuable insights into how firms perceive the costs and benefits of cybersecurity measures, shaping their investment decisions. The economics of cybersecurity explores how businesses allocate resources to protect their information assets, often weighing the potential costs of cyberattacks against the expenses associated with implementing robust security measures.

2.2.1 Cost-benefit analysis

Businesses often invest in cybersecurity in response to the costs associated with cyber breaches (Shaikh and Siponen, 2023). The financial repercussions of such breaches include direct costs such as legal fees, fines, and the expense of incident response, patching and reconfiguring systems, as well as indirect costs like loss of customer trust and brand reputation. The threat of loss can act as a significant motivator for businesses to enhance their cybersecurity measures and economic models such as the Gordon-Loeb model which measure potential loss from cyber-attacks are often used to guide organisations about how much to invest in digital security (Gordon, Loeb and Zhou, 2016).

However, it is challenging to identify an optimal level of investment with a cost-benefit analysis. The costs of implementing cybersecurity solutions are often immediate and substantial, while the benefits, such as risk reduction and enhanced security, are long-term and not fully internalized by individual firms. For example, in the case of new secure hardware adoption, Tomlinson, et al (2022) note a prevalence of short-termism in business decisions – companies would rather incur regular (if rising) operational expense towards cybersecurity rather than incur a large up-front capital expenditure to transitions towards a system with secure-by-design hardware and software systems. Moreover, cybersecurity can be considered a credence good, i.e., unlike traditional goods, the benefits of cybersecurity measures are not always visible or immediately apparent to users. The effectiveness of these measures is often only realized when a potential threat is thwarted, making it difficult for firms to gauge the true value of their investments.

2.2.2 Externalities and game theory

A firm's investment in cybersecurity can create both positive and negative externalities – more security investment can make other firms sharing a common network also more secure against indirect attacks, but more security investment by one firm can make it less attractive to attackers who would then direct their attention to other firms (Ezhei & Tork Ladani, 2020). The interconnected nature of the digital world further complicates the decision-making space for cybersecurity investment. Firms often share common networks or are part of supply chains, making them vulnerable to cyberattacks taking place in other parts of the system. This interdependence creates a scenario where cybersecurity becomes a collective good, requiring coordinated efforts to ensure comprehensive protection.

Game theory has been applied to understand cybersecurity investment in multi-firm settings, and features externalities or spillovers arising from sharing a common network or competing in the same market (Fedele and Roner, 2022). Game theoretic approaches point out that there may be a difference between socially efficient versus equilibrium or individual-level of cybersecurity investment by firms (Jianqiang, Shue and Weijun, 2015; Cerdeiro, Dziubiński and Goyal, 2017), which highlights the importance of cooperative strategies and shared investments in enhancing overall cybersecurity. For instance, collaborative frameworks, joint security protocols and shared investments in cybersecurity infrastructure could help in effectively managing the collective risks of cyber-attacks in an interdependent network.

2.2.3 Behavioural biases

Behavioural biases play a significant role in shaping cybersecurity investment decisions within firms. Optimism bias, for example, leads businesses to underestimate the likelihood and potential impact of cyberattacks on their organizations. This bias can result in insufficient investment in cybersecurity measures, as decision-makers may falsely believe their existing defences are adequate. Similarly, recency bias influences firms to prioritize cybersecurity investments based on recent, high-profile cyber incidents, potentially overlooking more comprehensive, long-term strategies.

A strong body of research on cybersecurity focusses on human behaviour and its impact of organisational preparedness and resilience to cyberattacks (Beautement, Sasse and Wonham, 2008; Crossler *et al.*, 2013; Ceric and Holland, 2019; Kweon *et al.*, 2021). This has resulted in a focus on employee training and cyber safety awareness campaigns, vis-à-vis techno-administrative measures like setting out organisational security policies and procedures (Merete Hagen, Albrechtsen and Hovden, 2008). However, the effectiveness of security training for behavioural changes is much less certain and is often conditional on several factors ranging from message framing to pedagogical approach (Chaudhary, 2024).

In the pedagogical space, serious games are increasingly being positioned as tools which can increase engagement with and awareness of cybersecurity issues, even among non-technical audiences (Hart *et al.*, 2020). This is especially useful to our research area as small businesses and start-ups may not always have the knowledge to effectively evaluate the effectiveness of cybersecurity technologies, as knowledge gaps exist even in cyber security graduates (Catal *et al.*, 2023), let alone the general public (Kostyuk and Wayne, 2021). Cybersecurity games have been shown to provide experiential and immersive learning environments (Cone *et al.*, 2007), involve active participation from the learners (Sheng *et al.*, 2007; Beckers and Pape, 2016), and often help to externalise the inherent beliefs, biases, and knowledge of players (Allal-Chérif, Bidan and Makhlouf, 2016). This means that games can be used for teaching as well as research on cybersecurity behaviours. A few researchers have applied games and simulations as research tools to unveil cognitive biases and decision-making processes, for example Safi and Browne (2023), Jalali *et al.* (2019), and Shreeve *et al.* (2020).

2.3 Research problem

While games have been used to understand digital security preferences and behaviours, to the best of our knowledge, cybersecurity games usually concentrate on information systems and digital security in isolation, overlooking potential trade-offs stemming from other priorities that a business may have such as growth, market competition, and productivity. Games and simulations also often presume a static security budget, neglecting the dynamic nature of resource allocation in real-world scenarios, and more importantly, tend to define a dedicated cybersecurity budget, which is an unlikely scenario in many small firms (Heidt, Gerlach and Buxmann, 2019).

The aim of this paper is to improve understanding about cybersecurity behaviours and secure technology adoption in small business and start-ups. Such entities face stronger budget constraints and must make trade-offs and choices about allocating their budget between product development, acquiring customers, and cybersecurity. Moreover, new security-related technologies may arrive on the market promising improved digital security, in response to the dynamic nature of the cyber threat landscape. Drawing on concepts from technology adoption literature and economics, it would be interesting to also explore how small businesses and start-ups approach new secure technologies. Thus, we have two research questions.

RQ1: What are the different investment strategies exhibited by start-ups, i.e., how is a dynamic budget allocated between product development, marketing, and cybersecurity?

RQ2: What are the factors which influence a start-up to adopt new secure technology?

We use a game-based simulation where players imagine themselves as founders of a digital start-up and allocate a dynamic budget towards different business needs, including cybersecurity. Our aim is to use the game to observe the trade-offs between cybersecurity and other business requirements and how this might affect technology adoption from an SME perspective. Since there also exists a rich literature about the use of games as an innovative pedagogical tool for raising cybersecurity

knowledge and awareness among non-technical groups, our third research question evaluates the role of the game for engagement as well. While this may suggest a departure from our core interest on small businesses and start-ups, the answer is nevertheless important to contextualise the role played the research tool, i.e., the game-based simulation, in building awareness and knowledge about cybersecurity among digital businesses and start-ups.

RQ3: How does game play affect players' interest and knowledge of cybersecurity in a business context?

3. Methods and data

3.1 Game design and mechanics

We are using a table-top boardgame which we have developed under the UKRI's Digital Security by Design initiative¹. Briefly, the game comprises of 12 “rounds” and is played cooperatively in teams of 2 to 4 players. Teams make decisions about allocating their budget across different business requirements like product development (referred to as “product innovation” in the game), marketing, and cybersecurity (Figure 2) in each round. In the game, marketing leads to customer acquisition only if the players roll their dice favourably. In early stages, it is very difficult to get customers, but the probability of marketing success improves over time, following the Diffusion of Innovation theory. Teams also have the option of spending money to ask questions from “The Cybersecurity Consultant”. Teams can also take a loan to expand their available cash.

At the end of a round, teams collect revenue from their customers (if any) and carry the remaining budget to the next round. For the first three rounds (‘first quarter’ in game play terms), teams can roll a dice and get a random investor who gives them some money as a ‘gift’. However, from the second quarter, teams receive capital from “The Auditor” based on their performance like how quickly they progress through the rounds, the size of their customer base, and outstanding loan payments, if any.



Figure 2 The game board

¹ Game webpage: <https://www.discribithub.org/boardgame-threats-tradeoffs>

Existing research on information systems management suggests that cybersecurity incidents act as “learning triggers” for firms (Weishäupl, Yasasin and Schryen, 2018), and in this game, teams experience cyberattacks at random across the 12 rounds. When “The Sentinel” approaches a team, a member of the team (player) rolls the dice. If the team rolls an even number, there is no cyberattack. However, if the team rolls an odd-number, “The Sentinel” rolls a 20-sided dice which contains a variety of cyberattack scenarios. We have used data from the ‘UK Cyber security breaches survey 2023’ to determine relative probabilities of cyberattacks (see Appendix Table A1). If a team has the appropriate cyber defences, they face no consequences. Otherwise, a cyberattack leads to financial losses and reputational damage. The game ends if a team’s reputation score falls below 1. The reputation score can be improved during a round by making an investment in the “satisfaction trackers”.

3.2 Game delivery and recording data from game play

Game play takes approximately 1 hour. Before the game, players are invited to complete a short quiz to assess their knowledge and perceptions about cybersecurity (see Appendix B). The introduction to the game features a non-binding round (the start-up incubator) where teams learn about game rules and can ask any clarifying questions. After the game, players complete the same quiz and the research team conducts a debriefing session to further consolidate player learning. Changes in learning are assessed by comparing the pre- and post-game quiz or survey responses, where each respondent uses a unique identification number to help with the matching and also to maintain anonymity.

The survey is one of the three sources of data being gathered in this study, and its main objective is to evaluate the effectiveness of the game as a teaching tool (RQ3). Survey responses also help us in characterising players and teams. Decisions made during game play are being recorded in a physical “player handbook” (Figure 3). Analysing the handbooks help us map team strategies and respond to RQ1 and RQ2. Data collection during the workshop also involves participant observation during the game play and the post-game debrief and discussion, which helps us to expand our response to the research questions. Thus, we use a mixed methods approach in our study. Ethical approval for this research was obtained from the university’s Research Ethics Committee².

ROUND 1

Starting budget: £0k. Roll the dice once to get money.

Fred	Angela	Barney	Axel	Cora	Vincent
£6k	£8k	£8k	£12k	£20k	£20k

We are feeling: (place a tick-mark) 😊 😎 😐 😞 😫 😡

We can take a **loan** from 0 upto the current budget. Loan amount: £ k

Money available: £ k (current budget + loan amount)

Expenditure

Product Innovation (INVEST +)

Seek help from **The Consultant**

Also add the investment to the **product innovation tracker**.

Antivirus (employees)	£2k	Buy
Antivirus (doctors)	£2k	Buy
MFA (employees)	£2k	Buy
MFA (doctors)	£2k	Buy
Standard reader	£4k	Buy
Data backup	£4k	Buy
DDoS protection	£4k	Buy
Web portal whitelisting	£4k	Buy
Intrusion prevention system	£8k	Buy
Security training (employees)	£8k	Buy
Security training (doctors)	£8k	Buy
Secure by design reader	£10k	Buy

Marketing (You get 1 customer only if you roll 1 on the dice.)

END OF ROUND 1

Customer revenue: Multiply total customers with product price. The product price is based on your stage (check product innovation tracker).

Cyber update: When total customers crosses 5, 10, and 15, you must repurchase your reader device and cyber defences.

Loan payment: Consult Page 1 and your Loan Pad for information.

Total customers:

Category	Money in	Money out
Investment received		
Loan taken		
Product innovation		
Reader device		
Cybersecurity		
Consultancy		
Marketing		
Customer revenue		
Cyber update		
Loan payment		
Cyberattack		
Total		

Budget: £ k
(total 'money in' - total 'money out')

Figure 3 Sample page from the player handbook

² University of Bath ethics application reference number: 0846-1393

3.3 Data collection

For the purposes of this paper, we collected data by conducting 2 in-person game-based simulation workshops with participation from 37 postgraduate business and management students. We recognise the limitation that our sample does not accurately represent the e-business and digital start-up community as students often do not have real-world business experience (Table 2 shows the responses of workshop participants to a question on professional experience). However, it can be argued that business and management students represent future entrepreneurs and business leaders. Moreover, our research is in its early stages with continuous iteration and development of the game itself, based on playtests and user-feedback. We are improving and streamlining the game so that it can be played more easily by people who are more time-constrained like working professionals in small businesses and start-ups.

Table 2 Question in pre-game quiz ‘Do you have any prior experience of managing a business?’

Response	Number of respondents
Yes, I have extensive experience of managing my own business	0
Yes, I have some experience of managing a business as part of a team or in a leadership role	12
No, but I have worked closely with business managers or entrepreneurs in my professional career	14
No, I have no direct experience of managing a business or working with business managers	7
No, I have no prior professional experience in the world of business	4

The workshops were held in March 2024 – the first workshop involved 23 participants who arranged themselves in 5 teams of three and 2 teams of four, the second workshop involved 14 participants who arranged themselves in 7 teams of two. Therefore, we have game play information from 14 teams in total. In terms of duration, both workshops were 3.5 hours long (including the pre-game and post-game survey) and were conducted on university premises during normal working hours.

4. Findings

We analyse three forms of data: (1) participant survey conducted before and after game play, (2) game play as recorded in the player handbook (Figure 3), and (3) observations and notes made by a member of the research team during the game sessions. Combining these three sources of information allows us to respond to our three research questions in a more comprehensive manner.

4.1 Budget allocation and investment profiles

Our first research question is about investment strategies. The two workshops make it possible to observe the game play strategies of 14 teams over successive game rounds. We used a discrete mixture model to model this longitudinal data and identify longitudinal latent classes or data groups (Jones and Nagin, 2013) based on budget allocation across three categories – cybersecurity, marketing, and product innovation. We found three clusters, i.e., three types of budget allocation strategies (Figure 4). There were no dominant strategies – teams are roughly equally distributed across the three strategies, although this may change when we gather more data by conducting more game workshops.

The three groups exhibit similar strategies with respect to cybersecurity – there is a large up-front investment in cybersecurity in the early stages which declines over time. Group 1 (31% of the teams, blue dots) show a steady accumulative tendency while Group 3 (32.3% of the teams, green dots) make a large investment in Round 1, avoid cybersecurity investment in Round 2 (perhaps to observe its effects), and then make incremental investments in cybersecurity. Where the groups distinguish themselves is in their approach to marketing. Group 3 spend a larger portion of their budget that other groups in marketing which helps to acquire customers in the game. Since customer acquisition is

determined by the roll of a dice, it may be the case that teams in Group 3 were particularly unlucky with their dice rolls. In contrast, Group 2 (36.6% of the teams, red dots) and Group 1 spend a smaller share of their overall budget in the game on marketing. Group 1 has an almost Gaussian distribution, with marketing taking up a larger share of budget as the game progresses to its halfway point and falling afterwards. However, Group 2 shows a steady decline in the share of budget allocated towards marketing. In terms of product innovation spending, we again find the groups differing, with Group 1 and 2 having a decreasing share of budget allocation towards product innovation over time but Group 3 increasing its budget share towards this spend category as the game progresses.

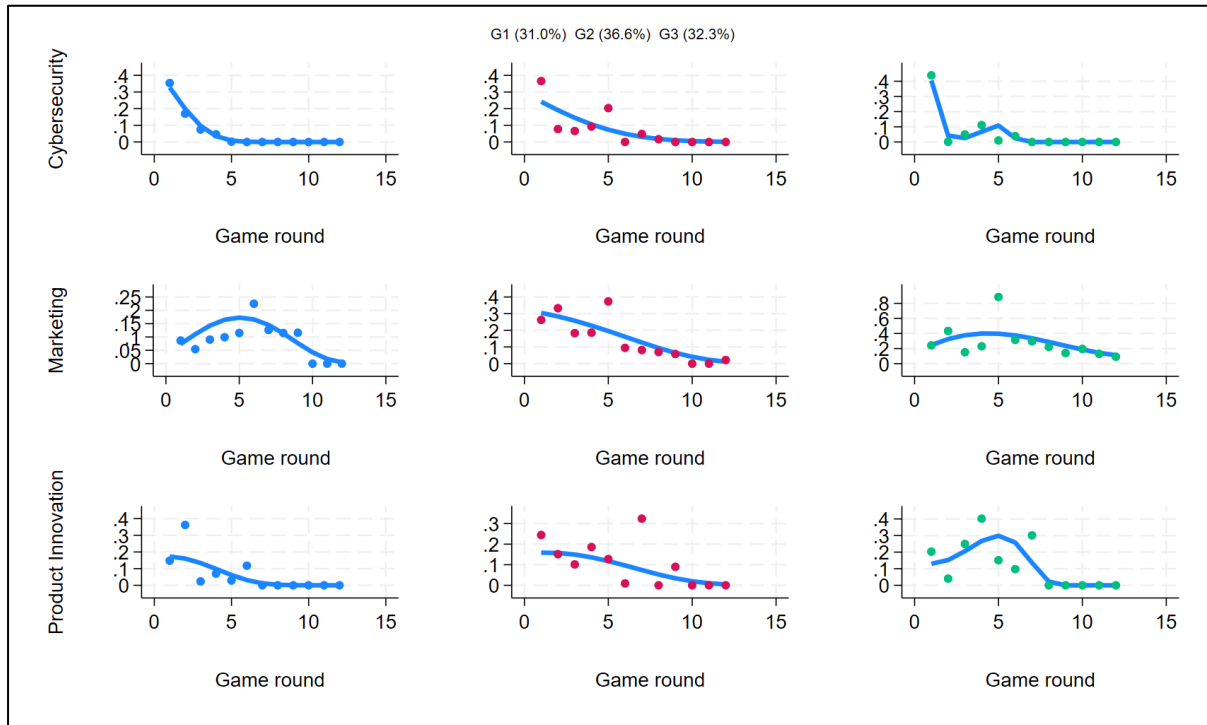


Figure 4 Relative spending (share of available funds) allocated across three spend categories over game rounds.

One of the main motivators for investing in cybersecurity was the fear of cyberattacks, rather than any inherent value of cybersecurity itself. A fixed effects regression reveals that a cyberattack in the previous round has a significant effect on cybersecurity spending in the next round (Table 3). This demonstrates a strong recency bias, i.e., recent events have a strong effect on budget allocation towards cybersecurity.

Table 3 Fixed effects regression (dependent variable: cybersecurity spending in a round)

VARIABLES	(1)	(2)	(3)	(4)
Cyber-attack in the last round (=1)	2.783*	2.726*	2.956*	2.679
	[1.270]	[1.277]	[1.366]	[1.373]
Cyber-attack in the penultimate round (=1)			0.126	-0.004
			[1.412]	[1.411]
Funds at the start of the round		-0.000		-0.000
		[0.006]		[0.006]
Accumulated customers		-0.085		-0.134
		[0.116]		[0.130]

Constant	1.727*** [0.474]	2.493** [0.826]	1.753** [0.604]	3.185** [1.108]
Observations	87	87	73	73
R-squared	0.063	0.080	0.079	0.118
Number of teams	14	14	14	14
Statistical power	0.453	0.809	0.288	0.750

Standard errors in brackets; *** p<0.001, ** p<0.01, * p<0.05

More generally, we observed that even when teams were unsure about cyber-related aspects of the game and its impact on running the business, there was a tendency to focus on customer acquisition and product innovation (things they were familiar with) in group discussions. Teams rarely chose the consultancy option and when they did, they asked questions about which specific cyber defences would protect the business against most cyber-attacks, thereby trying to get the most defence from smallest cost. An increase in spending on cybersecurity after a cyberattack does not come at the expense of spending on other categories. Teams were generally aiming towards preserving liquidity to ensure that the business could survive the financial cost of a cyber-attack.

4.2 Decision to adopt new cyber-secure technology

In the game, a ‘reader device’ is the main product-service offering of the start-up and teams can choose between two types of readers – a ‘standard reader’ and a ‘secure by design reader’ which costs 2.5x more but provides additional security features by enhancing memory-safety at the hardware level. Our second research question focuses on the adoption of new cybersecurity technology by digital start-ups and small businesses. Amongst the 14 teams, only 4 teams chose the ‘secure by design’ reader. Two teams purchased the ‘secure by design’ reader from round 1 itself, and one of the teams remarked during the debrief session that their decision was motivated by some level of futures thinking (“we would have to buy it sooner or later”). Two other teams purchased the ‘secure by design’ reader device in Round 4, one of them right after they had faced a cyberattack on their reader device (‘DDoS attack on reader’).

More generally, what seems to distinguish teams in choosing a new secure technology like the ‘secure by design’ reader seems to be a matter of the investment received or their budget. A survival analysis of the ‘secure by design’ reader option shows that one more unit of investor funds, which augments budgets and increases loan taking capacity, leads to a 4.8% increase in the adoption of new technology (Table 4).

Table 4 Random effects parametric survival results – hazard ratios

	(1)	(2)
VARIABLES	Exponential distribution	Weibull distribution
Investment received	1.048* [0.019]	1.048* [0.021]
Loan	1.016 [0.013]	1.016 [0.013]
Constant	0.003 ***	0.003***

	[0.001]	[0.003]
Observations	101	101
Number of Teams	14	14

Robust standard errors in brackets; *** p<0.001, ** p<0.01, * p<0.05

Our small sample size limits our ability to perform statistical tests to identify differences between the three groups – those who adopted ‘secure by design’ reader in Round 1 (n = 2), those who adopt it in Round 4 (n = 2), and those who do not adopt it at all (n = 10). Nevertheless, we wanted to explore whether there were any team characteristics which played a role in technology adoption. We had conducted a survey in which participants were asked to rate their knowledge about cybersecurity, entrepreneurship, and confidence in managing a business on a scale of 1 to 10, where 1 is low and 10 is high. We performed Kruskal-Wallis test on the pre-game survey responses and found that the groups significantly differ in their self-reported measures of entrepreneurship and cybersecurity knowledge (Table 5). Teams which adopt ‘secure by design’ technology early in the game have the *highest* self-reported measure of entrepreneurship knowledge among the three groups and the *lowest* self-reported measure of cybersecurity knowledge (Table 6). This may suggest that an inherent entrepreneurial streak rather than technical knowledge plays a role in technology adoption.

Table 5 Kruskal-Wallis test results

VARIABLES	H-statistic	p-value
Entrepreneurship knowledge (pre-game)	8.21	0.016
Cybersecurity knowledge (pre-game)	8.91	0.012
Confidence in running a business (pre-game)	4.52	0.104

Table 6 Characteristics of groups (average scores)

Name	n	Entrepreneurship knowledge (pre-game)	Cybersecurity knowledge (pre-game)	Confidence in running a business (pre-game)
No adoption	10	4.7	4.37	4.45
Adoption in Round 4 (late adopters)	2	4	3.13	3.25
Adoption in Round 1 (early adopters)	2	6.84	2.17	3.84

4.3 Engagement and learning

Participants were asked about their familiarity with cybersecurity and entrepreneurship, and their confidence in managing a business using a scale ranging from 1 to 10 in both the pre-game and post-game surveys, with 1 representing low and 10 representing high ratings. To answer the third research question on impact of game play on learning, we calculated the difference between these self-reported

measures. The Shapiro-Wilk test of normality on the differences indicated non-normal distribution for the cybersecurity and confidence measures. We therefore conducted a non-parametric test of difference – the Wilcoxon signed-rank test.

We found significant improvement across all measures: entrepreneurship (statistic = 21.0, $p < 0.001$), cybersecurity knowledge (statistic = 13.5, $p < 0.001$), and confidence in running a business (statistic = 28.0, $p < 0.001$). This suggests that the game positively affected participants' self-reported entrepreneurship knowledge, cybersecurity knowledge, and confidence. Some players remarked that although they got a sense of cybersecurity through playing the game, there was “lots to take in” and the game did not really teach them the terminology and concepts of cybersecurity. We think this is a point where the game needs to be supplemented with more formal teaching of basic cybersecurity terms. The game helps in removing the entry barriers to learning by being “fun”, but it does not teach cybersecurity by itself.

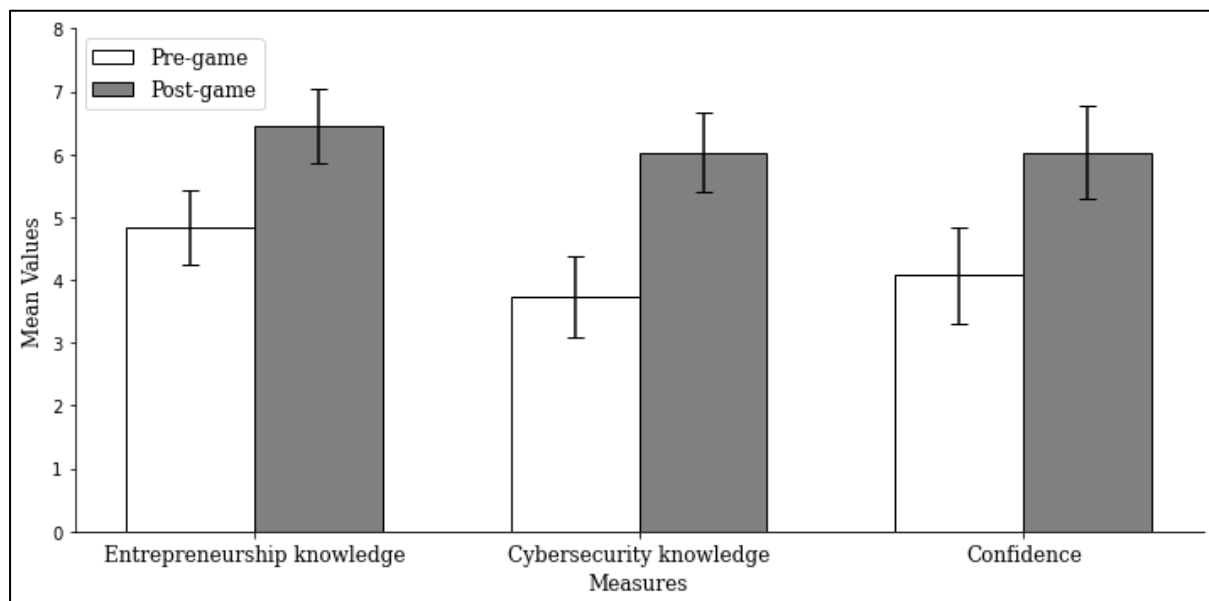


Figure 5 Changes in self-reported measures of learning before and after playing the game ($n = 37$)

In the post-game survey, we also asked participants if they would be willing to play the game again. The question offered 3 responses – “Yes”, “No”, and “Maybe”. 31 participants responded “Yes”, 5 responded “Maybe”, and there was 1 response for “No”. During the workshops, we observed a sense of excitement about the game during the introduction, particularly the prospect of cyberattacks, perhaps because cybersecurity was a new area of learning. While some players were unsure of how to proceed in the beginning, we noticed that players become more confident as they played and made progress over the rounds. We also observed some players intermingling and mixing with other teams (technically “competitors”) to understand the game better.

In one of the workshops, the post-game debrief session led to reflections of how decision-making would have been different if this was “real life”. A consensus emerged among the participants that legal regulations would have naturally led them to focus more on data security, but since this was not the case in the game, players’ treated data protection as optional in the early stages of the game. We think an interesting variation of the game would be in creating regulations around some of the cybersecurity measures (requirement to train employees and staff members, purchase secure-by-

design readers, enforce multi-factor authentication, and so on) and observe any differences in game play between those in a regulated environment and those in an unregulated environment³.

We conducted an analysis to investigate whether changes in self-reported knowledge and confidence correlate with participants' willingness to play the game again. To examine this relationship, we performed an ordinal logistic regression, treating the willingness to play again as the dependent variable and the changes in self-reported measures (differences between post- and pre-game scores) as independent variables. The model included changes in entrepreneurship knowledge, cybersecurity knowledge, and confidence as predictors.

The ordinal logistic regression analysis did not reveal significant associations between changes in entrepreneurship knowledge, cybersecurity knowledge, or confidence in running a business with the willingness to play the game again. However, the threshold for moving from "No" to "Maybe" was significant (coefficient = -2.6490, standard error = 1.130, $z = -2.345$, $p = 0.019$), indicating a clear distinction between participants who were unwilling and those who were uncertain about playing again. Overall, the results suggest that improvements in these self-reported measures do not significantly influence participants' likelihood of replaying the game, which is a good outcome since it indicates that there is willingness to play the game again irrespective of any sense of reward in terms of learning, which in any case may be a slow, cumulative process.

5. Discussion

Our paper explores cybersecurity behaviours and technology adoption in small businesses and start-ups using a game-based simulation. Small businesses and digital start-ups may be highly exposed to cyber threats but also face tough resource constraints. What types of investment strategies are adopted in the face of trade-offs? What determines the adoption of new secure technology? Existing research on technology adoption draws on psychological and economic factors. We find a combination of these at work in our workshops where 37 postgraduate business and management students took part in a game-based simulation where they were tasked with running a fictitious digital healthcare start-up.

5.1 Investment strategies

Our first research question explored the types of investment strategies employed by teams in the game. The analysis identified three distinct budget allocation strategies regarding cybersecurity, marketing, and product innovation. These strategies were roughly equally distributed amongst the teams with no dominant approach, indicating diverse financial management styles.

Across all three groups, a common pattern emerged of high initial investment in cybersecurity, which then tapered off over time. This suggests a recognition of the importance of establishing a strong security foundation early on, possibly driven by an awareness of the significant risks posed by cyber threats. Group 1, characterized by a steady cumulative investment in cybersecurity, may reflect a cautious and consistent approach to managing cyber risks. In contrast, Group 3's large initial investment followed by minimal spending in subsequent rounds might indicate a strategic evaluation period to assess the efficacy of their initial defences before committing additional resources. Where the groups strongly distinguish themselves in their share of budget allocation is on marketing and product innovation. The differing trends in spending reveal contrasting beliefs about growth and competitiveness, an area of greater discussion between teams perhaps drawing on their disciplinary background and knowledge.

This leads us to wonder whether investment strategies and the game would play out differently if we had a different group of people (e.g., computer science students, law students). We have a small

³ We would control for random chance between the two scenarios by subjecting teams to the same set of initial investment cards and the same sequence of cyber-attack cards.

dataset to draw upon at present and hope to expand this in later iterations of our research, particularly when we finish developing an online version of the game.

We also find recency bias plays a strong role in promoting investment in cybersecurity which leads us to conclude that cybersecurity adoption is driven by fear of losses rather than any inherent value in itself.

5.2 Technology adoption

The second research question addressed the adoption of new cybersecurity technology, specifically the decision to invest in a secure-by-design reader device. The adoption rate was relatively low, with only 4 out of 14 teams choosing the secure-by-design reader. This finding highlights a cautious approach towards high-cost security investments, despite the potential benefits.

The two teams that adopted the secure-by-design reader from the outset demonstrated a forward-thinking approach, possibly influenced by a strategic vision of future-proofing their operations. Interestingly, the teams had significantly lower self-reported measure of cybersecurity knowledge but higher self-reported measure of entrepreneurship knowledge. This paradox may indicate that entrepreneurial teams recognize the importance of purchasing cutting-edge security solutions, even if they lack technical cybersecurity expertise.

Survival analysis indicated that higher investor funding and increased loan capacity positively influenced the adoption of the secure-by-design reader. This suggests that financial flexibility and access to capital play crucial roles in enabling small businesses to invest in advanced cybersecurity solutions. Teams with constrained budgets may prioritize short-term survival over long-term security, highlighting the need for financial mechanisms that support strategic cybersecurity investments.

5.3 Game-based learning

The game provides a fun, interactive activity to explore business decisions for digital start-ups. The findings indicate significant improvements of students' self-assessment of entrepreneurial and cybersecurity knowledge, as well as confidence in running a business. These results highlight the game's effectiveness in providing experiential learning opportunities that translate into tangible improvements in participants' competencies. The interactive and immersive nature of the game likely contributed to these positive outcomes by engaging participants in realistic scenarios that require practical decision-making.

Participants' feedback indicated that while the game successfully conveyed the importance of cybersecurity, it did not adequately teach specific terminology and concepts. This gap suggests that the game should be supplemented with formal educational content to enhance its educational value. Additionally, the observed excitement and willingness to replay the game indicate its potential as a recurring educational tool that reinforces learning through repeated engagement.

Discussions during the debrief sessions revealed that participants would have prioritized data security more if the game included regulatory constraints. This insight suggests that integrating regulatory scenarios into the game could provide a more realistic and comprehensive understanding of the cybersecurity landscape. It also underscores the importance of regulatory awareness in shaping cybersecurity practices among future business leaders.

6. Conclusion

This paper investigates cybersecurity behaviours and technology adoption strategies in small businesses and start-ups through a game-based simulation. Our study stems from the pressing need to inform knowledge on how small businesses can navigate the dual challenges of significant cyber threats and constrained resources. By integrating psychological and economic theories of technology adoption with practical insights gained from a simulated business environment, our research contributes to a nuanced understanding of how small businesses approach cybersecurity investment and innovation.

The findings with a small sample of participants playing in teams reveal diverse investment strategies, although we do not observe strong differences in cybersecurity investment strategies. Initial high investments in cybersecurity, followed by a decline, aligns with economic theories such as the Gordon-Loeb model, which posits that firms will invest in cybersecurity up to the point where the marginal cost of additional investment equals the marginal benefit in terms of reduced risk. We also observe recency bias, where recent experiences heavily impact investment decisions, highlighting the psychological dimension of risk perception and decision-making.

Our examination of technology adoption, represented by the choice of reader device, underscores the cautious approach small businesses take toward high-cost security investments. This behaviour is consistent with the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT), which emphasize the role of perceived usefulness and ease of use in technology adoption decisions. The lower adoption rate observed in our study overall, but with higher adoption among teams with higher entrepreneurial knowledge suggests that a certain element of entrepreneurial drive may accelerate the adoption of new secure technologies.

The game-based simulation proved to be an effective educational tool, significantly improving participants' knowledge and confidence in entrepreneurship and cybersecurity. This finding supports the growing body of literature on experiential learning, which advocates for interactive and immersive educational methods to enhance practical skills and decision-making capabilities. The feedback from participants indicates that while the game effectively conveys the importance of cybersecurity, it needs to be supplemented with formal educational content to cover specific terminology and concepts more comprehensively.

Our study is not without limitations. The participant sample, comprising postgraduate business and management students, may not fully represent the broader population of small business owners and start-up founders. Additionally, we are still at exploratory stages and have not collected a large volume of data to make generalisable findings. We are continuing to receive feedback from playtesting on how to make the game more realistic. For example, expanding the game to include regulatory constraints could provide deeper insights into investment strategies and decision-making. We are also keen to create interconnected networks and dependencies to observe decision-making when faced with positive and negative externalities. Game-based simulations offer existing possibilities for future research. For example, we could observe whether investment strategies and learning outcomes vary by participant background. The development of an online version of the game could facilitate wider participation and the collection of more extensive data.

References

- Ajzen, I. (1991) 'The theory of planned behavior', *Organizational Behavior and Human Decision Processes*, 50(2), pp. 179–211. Available at: [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T).
- Allal-Chérif, O., Bidan, M. and Makhoul, M. (2016) 'Using serious games to manage knowledge and competencies: The seven-step development process', *Information Systems Frontiers*, 18(6), pp. 1153–1163. Available at: <https://doi.org/10.1007/s10796-016-9649-7>.
- Anvik, J., Cote, V. and Riehl, J. (2019) 'Program Wars: A Card Game for Learning Programming and Cybersecurity Concepts', in *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*. New York, NY, USA: Association for Computing Machinery (SIGCSE '19), pp. 393–399. Available at: <https://doi.org/10.1145/3287324.3287496>.
- Beautement, A., Sasse, M.A. and Wonham, M. (2008) 'The compliance budget: managing security behaviour in organisations', in *Proceedings of the 2008 New Security Paradigms Workshop*. New York, NY, USA: Association for Computing Machinery (NSPW '08), pp. 47–58. Available at: <https://doi.org/10.1145/1595676.1595684>.
- Beckers, K. and Pape, S. (2016) 'A Serious Game for Eliciting Social Engineering Security Requirements', in *2016 IEEE 24th International Requirements Engineering Conference (RE)*. 2016

IEEE 24th International Requirements Engineering Conference (RE), pp. 16–25. Available at: <https://doi.org/10.1109/RE.2016.39>.

BEIS *et al.* (2022) *National AI Strategy*. Available at: <https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version> (Accessed: 18 February 2024).

Burns, A.J., Posey, C. and Roberts, T.L. (2021) ‘Insiders’ Adaptations to Security-Based Demands in the Workplace: An Examination of Security Behavioral Complexity’, *Information Systems Frontiers*, 23(2), pp. 343–360. Available at: <https://doi.org/10.1007/s10796-019-09951-9>.

Catal, C. *et al.* (2023) ‘Analysis of cyber security knowledge gaps based on cyber security body of knowledge’, *Education and Information Technologies*, 28(2), pp. 1809–1831. Available at: <https://doi.org/10.1007/s10639-022-11261-8>.

Cerdeiro, D.A., Dziubiński, M. and Goyal, S. (2017) ‘Individual security, contagion, and network design’, *Journal of Economic Theory*, 170, pp. 182–226. Available at: <https://doi.org/10.1016/j.jet.2017.05.006>.

Ceric, A. and Holland, P. (2019) ‘The role of cognitive biases in anticipating and responding to cyberattacks’, *Information Technology & People*, 32(1), pp. 171–188. Available at: <https://doi.org/10.1108/ITP-11-2017-0390>.

Chaudhary, S. (2024) ‘Driving behaviour change with cybersecurity awareness’, *Computers & Security*, 142, p. 103858. Available at: <https://doi.org/10.1016/j.cose.2024.103858>.

Cone, B.D. *et al.* (2007) ‘A video game for cyber security training and awareness’, *Computers & Security*, 26(1), pp. 63–72. Available at: <https://doi.org/10.1016/j.cose.2006.10.005>.

Connolly, T.M. *et al.* (2012) ‘A systematic literature review of empirical evidence on computer games and serious games’, *Computers & Education*, 59(2), pp. 661–686. Available at: <https://doi.org/10.1016/j.compedu.2012.03.004>.

Crossler, R.E. *et al.* (2013) ‘Future directions for behavioral information security research’, *Computers & Security*, 32, pp. 90–101. Available at: <https://doi.org/10.1016/j.cose.2012.09.010>.

Davis, F.D. (1989) ‘Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology’, *MIS Quarterly*, 13(3), pp. 319–340. Available at: <https://doi.org/10.2307/249008>.

DCMS (2022) *UK Digital Strategy*. Available at: <https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy> (Accessed: 18 February 2024).

Denning, T. *et al.* (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*. New York, NY, USA: Association for Computing Machinery (CCS ’13), pp. 915–928. Available at: <https://doi.org/10.1145/2508859.2516753>.

DSIT and Home Office (2024) *Cyber security breaches survey 2024*. Available at: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024> (Accessed: 21 June 2024).

Ezhei, M. and Tork Ladani, B. (2020) ‘Interdependency Analysis in Security Investment against Strategic Attacks’, *Information Systems Frontiers*, 22(1), pp. 187–201. Available at: <https://doi.org/10.1007/s10796-018-9845-8>.

Fedele, A. and Roner, C. (2022) 'Dangerous games: A literature review on cybersecurity investments', *Journal of Economic Surveys*, 36(1), pp. 157–187. Available at: <https://doi.org/10.1111/joes.12456>.

Fishbein, M. and Ajzen, I. (1975) *Belief, attitude, intention and behaviour: An introduction to theory and research*.

Gordon, L.A., Loeb, M.P. and Zhou, L. (2016) 'Investing in Cybersecurity: Insights from the Gordon-Loeb Model', *Journal of Information Security*, 7(2), pp. 49–59. Available at: <https://doi.org/10.4236/jis.2016.72004>.

Hart, S. *et al.* (2020) 'Riskio: A Serious Game for Cyber Security Awareness and Education', *Computers & Security*, 95, p. 101827. Available at: <https://doi.org/10.1016/j.cose.2020.101827>.

Hasani, T. *et al.* (2023) 'Evaluating the adoption of cybersecurity and its influence on organizational performance.', *SN business & economics*, 3(5), p. 97. Available at: <https://doi.org/10.1007/s43546-023-00477-6>.

Heidt, M., Gerlach, J.P. and Buxmann, P. (2019) 'Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments', *Information Systems Frontiers*, 21(6), pp. 1285–1305. Available at: <https://doi.org/10.1007/s10796-019-09959-1>.

Huang, K. *et al.* (2023) 'The Devastating Business Impacts of a Cyber Breach', *Harvard Business Review*, 4 May. Available at: <https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach> (Accessed: 29 February 2024).

Illingworth, S. and Wake, P. (2021) 'Ten simple rules for designing analogue science games', *PLOS Computational Biology*, 17(6), p. e1009009. Available at: <https://doi.org/10.1371/journal.pcbi.1009009>.

Jalali, M.S., Siegel, M. and Madnick, S. (2019) 'Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment', *The Journal of Strategic Information Systems*, 28(1), pp. 66–82. Available at: <https://doi.org/10.1016/j.jsis.2018.09.003>.

Jianqiang, G., Shue, M. and Weijun, Z. (2015) 'Analyzing information security investment in networked supply chains', in *2015 International Conference on Logistics, Informatics and Service Sciences (LISS)*. *2015 International Conference on Logistics, Informatics and Service Sciences (LISS)*, pp. 1–5. Available at: <https://doi.org/10.1109/LISS.2015.7369701>.

Jones, B.L. and Nagin, D.S. (2013) 'A Note on a Stata Plugin for Estimating Group-based Trajectory Models', *Sociological Methods & Research*, 42(4), pp. 608–613. Available at: <https://doi.org/10.1177/0049124113503141>.

Kostyuk, N. and Wayne, C. (2021) 'The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public', *Journal of Global Security Studies*, 6(2), p. ogz077.

Kweon, E. *et al.* (2021) 'The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence', *Information Systems Frontiers*, 23(2), pp. 361–373. Available at: <https://doi.org/10.1007/s10796-019-09977-z>.

Lunceford, B. (2009) 'Reconsidering Technology Adoption and Resistance Observations of a Semi-Luddite', *Explorations in Media Ecology*, 8(1), pp. 29–48. Available at: https://doi.org/10.1386/eme.8.1.29_1.

- Makridis, C.A. (2021) 'Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018', *Journal of Cybersecurity*, 7(1), p. tyab021. Available at: <https://doi.org/10.1093/cybsec/tyab021>.
- Merete Hagen, J., Albrechtsen, E. and Hovden, J. (2008) 'Implementation and effectiveness of organizational information security measures', *Information Management & Computer Security*, 16(4), pp. 377–397. Available at: <https://doi.org/10.1108/09685220810908796>.
- Oliveira, T., Thomas, M. and Espadanal, M. (2014) 'Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors', *INFORMATION & MANAGEMENT*, 51(5), pp. 497–510. Available at: <https://doi.org/10.1016/j.im.2014.03.006>.
- Posey, C. *et al.* (2013) 'Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors', *MIS Quarterly*, 37(4), pp. 1189–1210.
- Rogers, E.M. (1962) *Diffusion of Innovations*. 1st Edition. New York, NY, US: The Free Press.
- Safi, R. and Browne, G.J. (2023) 'Detecting Cybersecurity Threats: The Role of the Recency and Risk Compensating Effects', *Information Systems Frontiers*, 25(3), pp. 1277–1292. Available at: <https://doi.org/10.1007/s10796-022-10274-5>.
- Shaikh, F.A. and Siponen, M. (2023) 'Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions', *Information Systems Frontiers* [Preprint]. Available at: <https://doi.org/10.1007/s10796-023-10404-7>.
- Sheng, S. *et al.* (2007) 'Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish', in *Proceedings of the 3rd symposium on Usable privacy and security*. New York, NY, USA: Association for Computing Machinery (SOUPS '07), pp. 88–99. Available at: <https://doi.org/10.1145/1280680.1280692>.
- Shreeve, B. *et al.* (2020) "'So if Mr Blue Head here clicks the link..." Risk Thinking in Cyber Security Decision Making', *ACM Transactions on Privacy and Security*, 24(1), p. 5:1-5:29. Available at: <https://doi.org/10.1145/3419101>.
- Taherdoost, H. (2018) 'A review of technology acceptance and adoption models and theories', *Procedia Manufacturing*, 22, pp. 960–967. Available at: <https://doi.org/10.1016/j.promfg.2018.03.137>.
- Tomlinson, A., Parkin, S. and Shaikh, S.A. (2022) 'Drivers and barriers for secure hardware adoption across ecosystem stakeholders', *Journal of Cybersecurity*, 8(1), p. tyac009. Available at: <https://doi.org/10.1093/cybsec/tyac009>.
- Venkatesh, V. *et al.* (2003) 'User acceptance of information technology: toward a unified view', *Management Information Systems Quarterly*, 27(3), pp. 425–478. Available at: <https://doi.org/10.2307/30036540>.
- Venkatesh, V. and Bala, H. (2008) 'Technology Acceptance Model 3 and a Research Agenda on Interventions', *Decision Sciences*, 39(2), pp. 273–315. Available at: <https://doi.org/10.1111/j.1540-5915.2008.00192.x>.
- Venkatesh, V. and Davis, F.D. (2000) 'A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies', *Management Science*, 46(2), pp. 186–204. Available at: <https://doi.org/10.1287/mnsc.46.2.186.11926>.

Weishäupl, E., Yasasin, E. and Schryen, G. (2018) 'Information security investments: An exploratory multiple case study on decision-making, evaluation and learning', *Computers & Security*, 77, pp. 807–823. Available at: <https://doi.org/10.1016/j.cose.2018.02.001>.

Wendt, C. *et al.* (2022) 'Let's Connect to Keep the Distance: How SMEs Leverage Information and Communication Technologies to Address the COVID-19 Crisis', *Information Systems Frontiers*, 24(4), pp. 1061–1079. Available at: <https://doi.org/10.1007/s10796-021-10210-z>.

Yadegari, M., Mohammadi, S. and Masoumi, A.H. (2022) 'Technology adoption: an analysis of the major models and theories', *Technology Analysis & Strategic Management*, 0(0), pp. 1–15. Available at: <https://doi.org/10.1080/09537325.2022.2071255>.

Younis, Y.A. and Alghamdi, M.Y. (2021) 'The use of computer games for teaching and learning cybersecurity in higher education institutions', *Journal of Engineering Research*, 9(3A). Available at: <https://doi.org/10.36909/jer.v9i3A.10943>.

Appendix A: selected game elements

Table A1 Cyber attacks in the game corresponding to The Sentinel's D20 dice

D20 roll	Cyber-attack	Description
1	Supply chain attack	There has been a cyber-attack on your pill supplier. Unfortunately, there was no way for you to prevent this attack, but the attack has a carry-over consequence for you.
2	Zero-day attack	An attacker scanned your application code and discovered a zero-day vulnerability, which they abused to trigger a fake update on customers' apps. The update installed malware that stole customer financial data and login credentials.
3	Black hat attack	A black hat breaks into your reader device, exploiting a memory vulnerability and causing it to malfunction.
4	Industrial sabotage	A competitor pays a cyber-crime facilitator to exploit memory-based vulnerabilities in your reader devices and causes them to malfunction.
5	Data exfiltration	An attacker finds a memory-based vulnerability in your reader devices, exfiltrates data from a large number of devices and sells it on a dark web. A cybersecurity researcher finds this data and informs you and the government.
6	DDoS through reader device	An attacker finds a memory-based vulnerability in your reader devices and exploits it to execute a DDoS attack from the devices' IP addresses
7	DDoS attack on the cloud	An attacker executes a DDoS attack on your cloud.
8, 9, 10	Phishing/ ransomware attack on employees	An attacker sends out phishing emails with a malicious link to your employees. A senior employee clicks on the link, activating the ransomware that blocks access to the key components of your network.
11, 12, 13	Phishing/ ransomware attack on doctors	An attacker sends out phishing emails with a malicious link to your doctors. A doctor clicks on the link, activating the ransomware that blocks access to the key components of your network.
14, 15	MITM / IP theft	One of your employees has been working from a coffee shop using insecure public wifi. An attacker has made a connection to your employee's device and managed to steal sensitive information that he used to obtain your company's IP, which he later sold to a competitor. Some of your customers switched to your competitors' services.
16	SQL injection/ Data theft	An attacker uses a vulnerability in your web portal to make an SQL injection and steal patients' data. A cybersecurity researcher finds the data on the dark web and reports the data breach to the authorities.
17, 18	Social engineering attack on doctors	An attacker executes a pretexting social engineering attack on one of your doctors, obtains their credentials, and steals sensitive patient data.
19, 20	Social engineering attack on employees	An attacker executes a pretexting social engineering attack on one of your doctors, obtains their credentials, and steals sensitive patient data.

Appendix B: questionnaires

Pre-game questionnaire:

https://docs.google.com/forms/d/e/1FAIpQLSdpyk01kFSJlk0I4MVVg0lSh8UwFn5UcdnbDxF63hZe0wzq1g/viewform?usp=sf_link

Post-game questionnaire:

https://docs.google.com/forms/d/e/1FAIpQLSfQQ3tw3bDSuI2bEaLjkMbA7CX_aTQG1HAe7yFf_oKzCVTToQ/viewform?usp=sf_link