DOI: http://dx.doi.org/10.14236/ewic/ICS2016.10

Using Gamification to Raise Awareness of Cyber Threats to Critical National Infrastructure

Allan Cook
Cyber Security Centre,
De Montfort University,
Leicester, LE1 9BH, UK
www.dmu.ac.uk
allan.cook@my365.dmu.ac.uk

Richard Smith
Cyber Security Centre,
De Montfort University,
Leicester, LE1 9BH, UK
www.dmu.ac.uk
rgs@dmu.ac.uk

Leandros Maglaras
Cyber Security Centre,
De Montfort University,
Leicester, LE1 9BH, UK
www.dmu.ac.uk
leandros.maglaras@dmu.ac.uk

Helge Janicke
Cyber Security Centre,
De Montfort University,
Leicester, LE1 9BH, UK
www.dmu.ac.uk
heljanic@dmu.ac.uk

Senior executives of critical national infrastructure facilities face competing requirements for investment budgets. Whilst the impact of a cyber attack upon such utilities is potentially catastrophic, the risks to continued operations from failing to upgrade ageing infrastructure, or not meeting mandated regulatory regimes, are considered higher given the demonstrable impact of such circumstances. As cyber attacks on critical national infrastructure remain low-frequency events, there is little to motivate business leaders to increase their investment in cyber defences to comparable levels. This paper describes SCIPS, a gamified environment in which senior executives experience the impact of a cyber attack on an electric power generation plant, demonstrating how it can strategically affect shareholder value, and allows them to form their own views on the relative importance of cyber security investment.

ICS, SCADA, Risk, HILF, Cyber, Security, Electric Power, Critical National Infrastructure

1. INTRODUCTION

A 2015 analysis of the impact of a malware infection on the US national grid demonstrated the potential for financial losses of between USD 243bn and USD 1trn. Despite such a compelling example, investment in the cyber security of industrial control systems (ICS) that underpin electric power and other elements of critical national infrastructure (CNI), remains low. This is, in part, due to the levels of investment required (Naedele (2007)) and the complexity of defending proprietary technologies (Stouffer et al. (2011)). In the case of electricity generation it is also due to the competition for budgets to support national power growth requirements, maintain existing infrastructure, improve supply reliability, and the transition to a smart grid (Kaplan (2009), Haught and Paladino (2012)), all of which generate a tangible return on investment and promote shareholder value. In contrast, expenditure to defend against ICS cyber attacks, which the North American Electric Reliability Corporation (NERC) (NERC (2010)) characterised as low-frequency events, does not demonstrate any immediately measurable benefits. Given the potentially catastrophic consequences of these high-impact low-frequency (HILF) cyber events, how do we raise the profile of security investment to safeguard against the threat?

Kaplan and Garrick (1981) propose that safeguards can be increased by raising awareness, arguing that by knowing that there is the possibility of a hazard, in this case a cyber attack, it poses less risk than if we have no understanding of its potential impact. In light of this, is it possible to create a situation in which senior executives within CNI organisations that operate ICS are presented with a credible threat scenario in order to raise their awareness and promote the prioritisation of cyber security investment?

2. GAMIFICATION

To generate the circumstances under which senior executives can experience the impact of a cyber attack to raise their awareness of the issues, we have 'gamified' a cyber incident, so that a series of events can be played out in a safe environment

that promotes self-learning. 'Gamification' is the process of using game mechanics and structures as a means to engage players in one or more problem-solving challenges, bound by rules, interactivity and feedback, to elicit an emotional reaction and result in a quantifiable outcome (Zichermann and Linder (2010), Kapp (2012)). Rieber (1996) highlights that games motivate participants intrinsically, encouraging them to draw their own conclusions as a result. Wolfe (1997) similarly comments that game-based approaches produce significant increases in knowledge over conventional learning methods, and promote motivation across different learning styles, whilst Kapp (2012) emphasises how game experiences can change a person's real-life perceptions.

Previous research into the gamification of cyber security education has focused on developing technical incident response skills rather than attempts to shift the perceptions of non-technical stakeholders impacted by such incidents (Fink et al. (2013), Boopathi et al. (2015)). Elements of response planning training by ENISA (2016) includes attempts to quantify the costs associated with cyber incidents, but does so at an operational level on IT systems, with financial impacts that could be mitigated through the purchase of insurance policies (Vaughan and Vaughan (2013)) and therefore potentially de-prioritised by an executive of a CNI facility facing competing demands for large-scale investment. In order to express the issues of cyber attack on CNI to the game's target audience the scenarios must illustrate an effect on the strategic viability of a critical infrastructure business and articulate the impacts in a lexicon familiar to C-level participants.

3. PROBLEM STATEMENT

To bound the scope and objectives of a gamified environment, a set of five overall high-level requirements were produced to guide the analysis and development process:

1. Produce an educational game targeted at high-level stakeholders to raise awareness of the business-level impact of cyber security incidents. The players will be assumed to have minimal ICS or IT security knowledge, but will understand the general objectives of a business.
2. The game and its purpose should be understandable in a reasonable amount of time (15 mins) and should not require detailed knowledge or previous experience.
3. The game should not follow a strict path and should keep the players focused on a scenario where there are no immediately apparent winning solutions.
4. The game should encourage debate within a team and promote competition between teams.
5. The game should allow the development of new scenarios and gameplay options, so that it can be repeated without significant re-working of the components.

To ensure the game was continually reviewed against its objectives it was decided it would be implemented using an iterative approach, within time-boxed development cycles, the first of which would be three-months in duration.

4. GAME DESIGN OPTIONS

4.1. Game Play

For the game to appeal to the target audience it was necessary to ensure that the nature of the gameplay lent itself to the players and the promotion of learning through self-discovery. An initial investigation reviewed the gameplay activity options defined by Kapp (2013):

Matching: In a matching game the player must match one item with another.
Collecting/Capturing: Where the goal is to acquire a certain number of objects. The player with the largest collection wins.
Allocating Resources: The player is required to balance the allocation of resources in order to achieve a working equilibrium. There is no competition with other players in this approach.
Strategising: A player allocates resources in a similar manner to an 'Allocating Resources' game, but is in competition with other players.
Building: Players try to create objects out of given materials.
Puzzle Solving: Players are required to solve a puzzle.
Exploring: Players interact with an environment looking for objects of value.
Helping: Involves one player assisting another player to accomplish a task.
Role Playing: The player assumes the role of another person, with their responsibilities defined within the confines of the game.

4.2. Game Medium

The medium of the game play was analysed against the learning objectives and problem statement, again using the definitions described by Kapp (2013):

Board Game: A turn-based approach with players moving around a pre-determined route through roles of dice.
Role Playing: A board-less, dice-based model where players interact with a facilitator who has a predetermined number of options for the players to explore.
Exercise: A scenario is presented with boundary conditions in which players can manoeuvre freely.
Single Player PC Game: An automated environment where players interact via a programmed interface with an algorithmic opponent.
Multi-Player PC Game: Similar to the single-player approach, but pitching player against player rather than an algorithm.

4.3. Game Design Approach

The gameplay and medium were considered in context together, resulting in the assessment matrix shown in Table 1. Whilst subjective, the matrix highlighted that *role playing* and *exercises* offered the closest fit to providing a platform on which to address the overall problem statement and learning objective. The decision was taken to combine the two approaches in an exercise format that requires players to adopt leadership roles typical of a critical infrastructure facility running ICS operations. In order to derive a scenario under which a cyber attack on a critical infrastructure facility would appear feasible, it was decided to construct a fictitious sequence of events based around UK foreign policy and military intervention in a fictitious country that has an indigenous offensive cyber capability (Wortzel (2013), Libicki (2009)). The resulting game was dubbed *SCIPS*, an acronym for "Simulated Critical Infrastructure Protection Scenarios."

5. PLAYER EXPERIENCE DESIGN PROCESS

To drive the gameplay through the player experience, a seven-step gamification development process from Burke (2014) was adopted. These steps, and the decisions taken therein, are described below.

5.1. Outcomes and Success Metrics

In the process defined by Burke (2014), the intended outcomes and measures of success must be defined at the outset to ensure the subsequent design steps adhere to the intentions of the game and the gamification experience. As such, it was defined that the intended outcome of playing the game would be that participants realise that:

1. There are circumstances under which a cyber attack could impact a CNI facility.
2. The drivers for the attack may come from actions beyond their control.

Figure 1: *The Player Design Experience Process (Burke (2014))*

3. Cyber attacks can have a direct impact on share price and shareholder value.
4. Investment in cyber security before an attack is the best way of preparing for this potential situation.

As the intended outcomes are aimed at a change in individual perceptions, the associated success metrics must be subjective. A player feedback sheet is completed at the end of the game that asks nine key questions, all scored using a consistent numeric range. The use of the feedback form allows participants to measure the shift in their understanding, and also to reinforce their changed perceptions through positive affirmation (Cialdini (2009)).

5.2. Target Audience

The game is intended for senior stakeholders within CNI organisations. Typically these should be participants who, during the course of their normal working activities, would have to balance investment decisions based on tangible outcomes and the needs of the business and shareholders.

5.3. Player Goals

In the SCIPS game, players are required to make a series of investment decisions based around the maintenance of a CNI facility that operates ICS equipment. In the initial version of the game this is based around an electric power generation plant. Subsequent implementations of the game are planned to address other industries within the CNI sector, supporting a broad spectrum of cyber-related scenarios.

Table 1: *Game Options Assessment Matrix*

	Board Game	**Role Playing (facilitated model)**	**Exercise**	**Single Player PC Game**	**Multi-Player PC Game**
Matching	*Gameplay did not lend itself to self-learning*	*Gameplay did not lend itself to self-learning*	*Gameplay did not lend itself to self-learning*	*Gameplay did not lend itself to self-learning*	*Gameplay did not lend itself to self-learning*
Collecting/ Capturing	*Gameplay was too focused on a predictable outcome*	*Gameplay was too focused on a predictable outcome*	*Gameplay was too focused on a predictable outcome*	*Gameplay was too focused on a predictable outcome*	*Gameplay was not viable in a head-to-head player environment*
Allocating Resources	*Difficult to allow players to allocate resources in a fixed board model*	**Viable: Players could adopt a role, but limiting the playing time and scope of decision making could prove difficult**	**Viable: Players could face a given scenario and attempt to reach equilibrium of resources. However, a non-competitive environment may not be appropriate for senior executives**	**Viable: Players could face a scenario, but the algorithm-based approach without other player interaction would limit opportunities for self-discovery**	**Viable: Players could face a scenario and play head-to-head. However, the computer environment would require game-playing literate competitors and may stifle debate**
Strategising	*Strategising on a board game tends to extend the time required to play*	**Viable: Although limiting the scope of the decisions available to players may prove challenging**	**Viable: Allows for competitive decision-making in a limited scenario. However, constraining the scope of the decisions to those appropriate to the game may prove challenging**	*The available development time would not fit into the project timescale*	*The available development time would not fit into the project timescale*
Building	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*
Puzzle Solving	*Gameplay lends itself to reaching a predetermined outcome, which is not appropriate*	*Gameplay lends itself to reaching a predetermined outcome, which is not appropriate*	*Gameplay lends itself to reaching a predetermined outcome, which is not appropriate*	*Gameplay lends itself to reaching a predetermined outcome, which is not appropriate*	*Gameplay lends itself to reaching a predetermined outcome, which is not appropriate*
Exploring	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*
Helping	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*	*Gameplay did not lend itself to problem statement*
Role Playing (assuming a role or persona)	*Role playing on a predefined board game did not appear feasible*	**Viable: Role playing would limit the scope of the decisions available to players, but overall game scope management would be challenging**	**Viable: Role playing would limit the scope of the decisions available to players, but overall game scope management would be challenging**	*The available development time would not fit into the project timescale*	*The available development time would not fit into the project timescale*

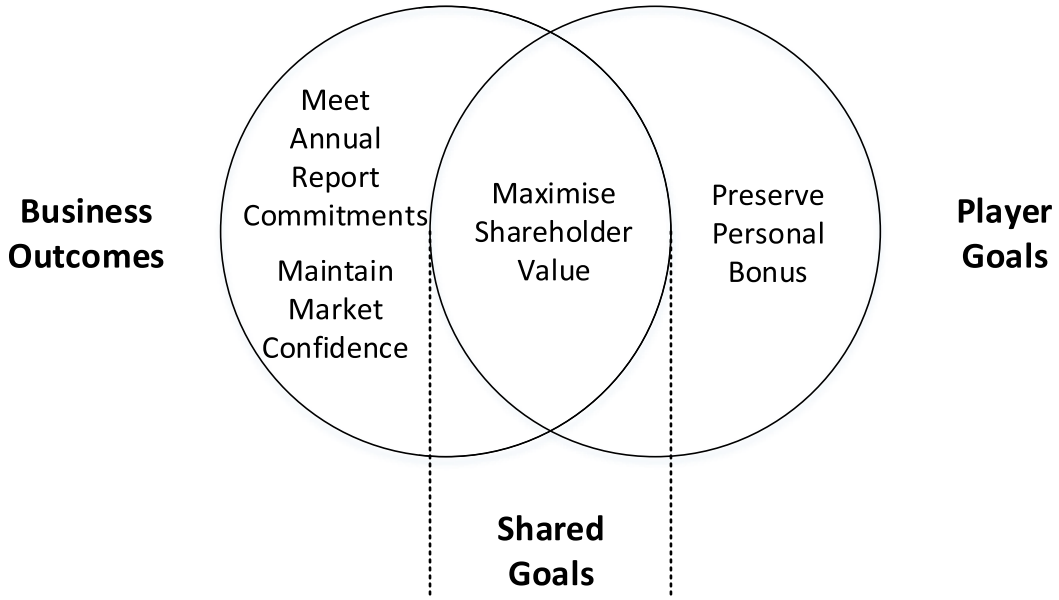

Figure 2: *SCIPS Player Goals*

Players are required to balance the competing priorities of shareholders and regulators with the security requirements to defend against a credible cyber threat. Each investment has a financial impact with associated trade-offs, but can protect revenues that result in maintained shareholder value. Players of the game adopt one of five roles within an organisation that operates a Combined Cycle Gas Turbine (CCGT) electricity generation plant. Their objective is to maximise shareholder value, expressed as share value and anticipated dividend per share. The winner is the team with the highest share value, and the loser is the CEO of the team with the lowest share value.

The business objectives of the game are to meet, as closely as possible, the investments stated in their annual report and to maintain market confidence. Figure 2 illustrates how the shared goal of each team is to maximise the share price, whilst individually, players try meet personal goals by preserving their bonuses which are impacted by the reallocation of funds within the business.

The exception to this is the Security Director. To create a player role who was more likely to champion the required security investments it was decided that the Security Director would have no bonus, and therefore have no external influences on their behaviours when considering the need for cyber protection mechanisms.

5.4. Engagement Model

Burke (2014) describes the ways that games engage with players in terms of positioning their gameplay in the following spectrums:

Collaborative to Competitive: The balance by which players are encouraged to adopt a 'winner-takes-all mentality' versus a collegiate approach to team success.
Intrinsic to Extrinsic: Defines how players are rewarded for their successes in the game.
Multiplayer to Solitary: The level to which players interact with each other, if at all.
Campaign to Endless: Describes the boundaries of the game, and whether it has a natural conclusion or can continue indefinitely.
Emergent to Scripted: Determines whether the outcome of the game is known, or evolves with the gameplay.

Figure 3 illustrates the current SCIPS engagement model, shown as black circles, and the extended engagement model that will be implemented in later versions of the game, as white.

The SCIPS game is essentially *collaborative* with intra- and inter-team *competitive* elements that drive debate between players about how to reallocate budgets in order to mitigate the cyber threat. Each round of the game is time constrained to drive instinctive behaviours from the executives participating (Menkes (2009)). A leader board is

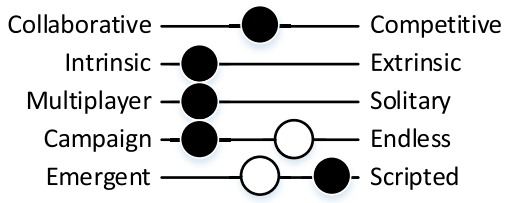

Figure 3: *SCIPS Player Engagement Model*

maintained throughout the game so that teams can see where their share price sits in respect to other teams.

Rewards within the game are *intrinsic*, focused on maintaining the fictitious organisations' financial targets and the personal compensation packages of the player roles within each team.

The game is *multiplayer*, with multiple players within teams, and multiple teams. Players primarily interact with the other members of their team, but are influenced by the financial performance of the other teams via the leader board.

The flow of the game follows a *campaign* that models a series of incidents based on a typical cyber attack 'kill-chain' (Hutchins et al. (2011)). Versions of the game planned for later releases will support a shift in gameplay towards an *endless* model based on attacker-defender (National Research Council (2010)) games that will support cyber warfare and 'capture the flag' functionality.

The current iteration of SCIPS is *scripted* to provide a credible scenario that leads to the cyber attacks. The initial version uses a US-UK coalition intervention in an overseas conflict to underpin the emerging cyber threat, and alternative scripted scenarios are also under development following a discussion between De Montfort University and CERT-UK (2015). Additionally, later versions of the game will support more emergent scenarios such as attacker-defender models.

5.5. Play Space and Journey

5.5.1. Play Space

The play space of the game is based around a game board, role cards, security cards, video feeds, newspaper 'cuttings', a tablet player interface and an overall leader board. All of the components of the play space interact, using a mix of soft and hard (physical) game play elements.

Game Board

The game board provides an illustration of a CCGT power plant to set the scene for the players, and to act as a focal point around which they can gather. It provides placeholders for purchased *security cards* to act as a quick reference for their increasing defensive capabilities.

Role Cards

The role cards, picked at random by the players, describe their responsibilities within the organisation and their compensation packages.

Chief Executive Officer (CEO): Ultimately responsible to the shareholders of the organisation and likely to see the cyber threat as an ongoing risk, but not an immediate priority that will affect the share value of the business.
Chief Operating Officer (COO): Responsible for the operations of the facility. The COO is likely to be aware of the possibility of a cyber threat, but likely to see the requirement for high availability and reliability as a higher priority issue.
Compliance Director: In regulated markets the Compliance Director will be responsible for ensuring that all regulatory and legal mandates are met. The role holder is not likely to focus on the cyber threat unless it corresponds to a stated requirement.
Plant Director: Responsible for the day-to-day operations of the facility and likely to report to the COO. The plant director will have detailed knowledge of the OT and the risk of any modifications or testing on plant operations. However, the Plant Director is also likely to be closer to the issues surrounding OT and the reality of the cyber threat.
Security Director: Responsible for IT and OT security and required to balance the management of both, although is unlikely to have the mandate to enforce changes on the operational environment.

Security Cards

The security cards within the game are configurable depending upon the scenario adopted. The initial version of the game uses the following:
External Firewalls: Protect the network perimeter and will limit the deployment of malware.
Email Filters: Detects potential phishing attempts.
Anti-Virus: Up-to-date and regularly updated anti-virus to contain attempts at malware propagation.
Intrusion Detection: Identifies abnormal behaviour on your network and servers and alert your systems administrators to potential malicious cyber activity.
Virtual Private Network: Securely extends the network to trusted business partners, preventing attackers from intercepting and manipulating data to deploy malware.
Deep Packet Inspection: Monitors the traffic flowing into and out of the network to identify malicious activity.
Risk Assessment: A comprehensive analysis of the threats to the business, their likelihood and subsequent impact on operations to quantify

the exposure the organisation has to service disruption through security incidents, and to allow the development of a qualified security plan.

Server Hardening: Disable all non-essential services on servers that expose known security vulnerabilities.

Patch Management: Initiates a programme to determine the current patch levels required for all devices and implement a pre-deployment environment to test them, ensuring they will not adversely affect operations.

Penetration Testing: Start an ongoing penetration test regime to regularly test the environment for security vulnerabilities.

Operational Technology (OT) De-Militarised Zone (DMZ): Install a DMZ between the IT and OT networks to minimise the risk of malware deployed in the IT environment propagating to industrial control systems.

Incident Response Process: Initiate an enterprise-wide programme to analyse the cyber threats to the business and develop plans to address them.

Segment IT Networks: Structure the IT networks of the organisation so that traffic is limited to the areas it needs to traverse, and limits the ability for malware to route to wider systems.

Create an IT/OT Security Team: Pull together a team of experienced professionals from both the IT and OT domains in order to consider and defend the organisations technology assets from cyber attack in a coordinated, holistic manner.

Profile OT Traffic: Initiate a programme of OT traffic capture and analysis so that intrusion detection systems can be configured to recognise abnormal activity on the OT network.

Limit User Account Permissions: Implement a policy of enforcing the least privileges required for each user account, so that users have access to the information they require, thereby limiting the ability of cyber attackers to access data and services.

Document Operational Processes: Produce a comprehensive set of documents that define the operational processes of the ICS systems and the control equipment that underpins them to determine which are critical to maintaining operational capability, and determine measures to mitigate the impact of their loss.

Limit External Accesses: Implement a processes of continual review of external accesses to the network so that connections are only permitted from trusted partners and only allowed to exist for the minimum time required.

Protect Designs: Identify all of the intellectual property and documentation key to the operational business and re-locate this to a repository where access is limited and audited.

Segment OT Networks: Structure the OT networks, buses and serial communications in a manner whereby the ability to traverse from one device or protocol to another can be limited, thereby restricting the ability of malware to propagate to ICS devices.

Configuration Management Processes: Introduce a set of processes to ensure that the configuration of all known devices is recorded, and any requests to modify them are properly assessed prior to changes being made.

Secure Operational Procedures: Implement a complete review of all operations across IT, OT and associated operations and develop policies for all aspects of personnel, processes and use of technology, then introduce programme of change to establish their use.

Catalogue Assets: Implement a programme to identify and catalogue all IT and OT assets within the organisation so that they can be properly managed.

Videos and Press Cuttings

At the beginning of each round a video is played to the teams via their tablet interfaces. It presents a simulated news broadcast that explains the initial scenario that will subsequently develop as the game progresses. The videos are supplemented by newspaper cuttings that summarise the news broadcasts so that players can refer back to salient points.

Tablet Player Interface

The players within the teams interact with the game and leader board through the tablet player interface. In the example screenshot in Figure 4, a team purchases security cards.

Figure 4: *An example of the tablet player interface (De Montfort University (2016))*

Leader Board

The game also uses a leader board that interacts with the tablet devices to display the financial positions of each of the teams, providing a comparative evaluation of their performance at the end of each round.

5.5.2. Journey
The journey that players experience through the game starts at *onboarding*, then progresses through the *game rounds* until the *game close* and the final *evaluation* of its effectiveness.

Onboarding
Prior to commencing the game, connectivity between the tablets and the leader board is established. At the start of the session players are introduced to the rules of the game by a facilitator. In later versions of the game this step will be automated and displayed on the tablet interface. Members of each team then pick a *role card* at random and enter their name against the role on the tablet.

Game Rounds
The game currently comprises six rounds, each representing a two-month period in a twelve-month financial year from April to March. In each round a new video broadcast is played to explain the ongoing situation in the fictitious country. In the first game scenario implemented, the players witness a UK-US coalition that employs economic sanctions and military intervention resulting in hacktivists from the region threatening to retaliate against UK energy infrastructure. The CEO of the fictitious company starts with his individual bonus reduced to 80 percent of its possible maximum value as a result of market sentiment reducing the team's company share price by 10 percent in response to the threat. After watching the video at the beginning of each round, players have a limited amount of time to decide which cyber security protection cards to purchase, and which of their existing budgets to transfer the funds from. Initially the scenario is baselined with none of the security cards selected, and a total investment budget available that is allocated between infrastructure, regulatory and generation upgrades. As the budgets are decremented, players can immediately see the impact on their overall share price and projected dividends to shareholders, as well as their own personal bonus. As the rounds progress, cyber incidents escalate from initial reconnaissance activity to effects against the energy production capabilities of the power plant, the impact of which can be limited by the purchase of security cards in previous rounds. Each of the security cards has four values assigned to it, used in the calculations regarding its impact:

1. Active?: This determines if the security card is active, based on the difference between its date of purchase and the current date, and the implementation timescale associated with the functionality.
2. Protection: Defines the maximum level of protection afforded by the security card.
3. Potential Impact: Defines the maximum impact that a cyber attack will have if that card is not purchased. This is defined as a numeric value and may be higher than the maximum Protection figure. This is to allow for realistic scenarios such as firewalls not detecting all attacks.
4. Actual Impact: If the security card is not active then this defaults to the Potential Impact figure, however if it is active then the value is set to the difference between the Potential Impact and Protection variables.

The Protection and Potential Impact figures change from round to round, as certain security cards afford better protection against each of the stages of the cyber attack. For instance, the Traffic Profiling security card in round 1 has no impact on preventing external IP network reconnaissance of the IT systems, whereas in subsequent rounds it offers the ability to detect traffic abnormalities in the OT space. The sum of all Actual Impacts of all of the security cards is calculated and a percentage presented back to the players to indicate how much, or little, their infrastructure was protected, as does a textual description of the impact. In later rounds of the first version of SCIPS, the summations of the Actual Impacts is divided by an impact factor to feed into the *cumulative impact of attacks* that reduces share price and impacts personal bonus figures.

Game Close: At the close of the game the players will have experienced the impacts of a cyber attack on the ICS in their power generation plant, the extent of which will have been limited, or not, by their cyber security investments. The leader board will display the overall performance of the teams, presenting the team with the highest share value as the winners, and the player in the role of CEO of the team with the lowest share price as the loser.

Evaluation: The purpose of the game is to change the perceptions of senior stakeholders in CNI organisations who possibly perceive investment in cyber security as an ongoing line on an IT budget that should be contained, to a strategic, top-line investment that protects shareholder value. Throughout the game, players develop their understanding of the impact of a well-executed cyber attack and form their own opinions as to the necessity of planned, defensive measures deployed in advance of such an incident. As players will come to the game with differing levels of experience and understanding of ICS and CNI, it is necessary to identify any shift in their views in order to evaluate the effectiveness of

the gamification. Players are encouraged to complete a feedback form that establishes their initial perceptions and measures any shifts in view as a consequence of the game. The questions asked include:

1. Before playing that game, what level of understanding of industrial control systems did you have?
2. Before playing the game did you consider the cyber security of industrial control systems to be a strategic issue?
3. The game presented players with a set of competing choices between corporate investment and personal bonus compensation. Do you consider that this was a realistic situation?
4. The game presented a cyber attack as a consequence of national foreign policy and use of military power overseas. Do you consider this to be a realistic scenario?
5. The security cards offered players the ability to increase specific areas of security, with associated costs and implementation timescales. Did the cards allow you consider the breadth of possible security investment?
6. Was the time taken to play the game appropriate?
7. Did you enjoy the game?
8. After playing the game do you agree that industrial control system cyber security is a strategic issue?
9. Did the game meet its objectives?

5.6. Game Economy

At the start of the game the players are presented with the investment budgets committed to in their fictitious company's annual report. These include provisions for upgrades to physical infrastructure, regulatory compliance, and power generation equipment. No provision was made for increased cyber security in their plans for the forthcoming financial year. To purchase security cards to protect their infrastructure, players must decrement these budgets to fund their investments. A reduction in committed inward investment results in the overall share price falling. Overall market sentiment (Kahn (2010)) is reflected in an initial 10 per cent fall in share price as a result of the threats by hacktivists, with further changes to market confidence as a result of investment decisions and public awareness of cyber attacks. Whilst trying to preserve the share price, players also try to maintain their personal bonus, which is also impacted by investment decisions, resulting in a tension between corporate and personal value.

5.7. Play, Test and Iterate

The game was initially implemented as a proof-of-concept demonstrator at De Montfort University (DMU) on 15th May 2015 to an audience of MSc students with no ICS or CNI experience. The player interface logic was modelled in a spreadsheet to allow for cross-variable relationships to be revised within short timescales if necessary. The aim of the initial game session was to identify any flaws in the logic or gameplay before presenting the concept to a senior audience. A revised version of the demonstrator was presented at Imperial College, London on 29th June 2015, attended by members of the Research Institute into Trustworthy Industrial Control Systems (RITICS), and a senior audience from government and industry. The feedback from the session was positive, although as the assembled audience were all involved in the cyber security of ICS there were no significant shifts in the perception of the importance of ICS cyber security. Following the presentation at Imperial College, DMU were invited to meet with CERT-UK 27th November 2015 to discuss new scenarios that could be developed in line with perceived threats to UK CNI.

The player interface is now under redevelopment as a tablet application, along with a more flexible game definition framework that allows new scenarios to be defined as configuration files. Support for team and player interactivity has also been improved so that later versions will allow attacker-defender models and 'capture the flag' competitions that will integrate with the DMU *'CYRAN'* cyber range.

6. CONCLUSIONS

Gamification is a proven method to change the perceptions and behaviours of players. Hamari et al. (2014), in a review of empirical studies on gamification, highlighted the positive effects it provides, but cautioned that its impact is highly dependent upon the context of the scenarios used and the backgrounds of the players involved. SCIPS has demonstrated its potential to influence a senior audience and present a plausible narrative in which a serious threat to UK CNI might emerge, articulating the impact in a language and economy familiar to business leaders. Further research is required to assess the impact of SCIPS across a broader range of audiences with differing levels of experience in strategic decision-making. This perspective is echoed by Stott and Neustaedter (2013) who point out that for gamification to be effective it must provide a realistic context for the players.

However, by presenting the players with the opposing requirements of maintaining share value whilst investing in cyber security, and preserving personal bonuses, players with and without strategic management experience have been observed to engage in detailed discussions about the priority of security investment versus the perceived cyber threat, and its context within the protection of shareholder value. As a result, SCIPS has met its objective of raising the profile of cyber security within ICS, and warrants further development to increase its range of impact.

7. FUTURE DIRECTION

SCIPS forms an essential element of ongoing DMU research into mitigating the risk of cyber attacks on ICS and CNI through the use of synthetic environments. The game's future direction will be guided by the strategic risk models developed as a consequence of this research, focusing on enterprise impact. The gameplay options will be extended to allow for greater interaction between teams and players, and include support for remote player options. However, as the game is intended to assist in changing the perceptions of senior executives, the game play will remain focused on providing the evidence necessary for its target audience to justify strategic investment in cyber security.

REFERENCES

Boopathi, K. et al. (2015). Learning cyber security through gamification. *Indian Journal of Science and Technology*, 8(7), 642–649.

Burke, B. (2014). *Gamify: How gamification motivates people to do extraordinary things*. Bibliomotion, Inc.

Cialdini, R. B. (2009). *Influence: Science and practice*, 4. Pearson Education Boston.

De Montfort University (2016, April). Scips user interface design.

De Montfort University and CERT-UK. (2015, Nov.) Meeting between de montfort university and cert-uk

ENISA. (2016) Trainings for cyber security specialists. https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/operational, [Accessed 25 April 2016].

Fink, G. et al. (2013). Gamification for measuring cyber security situational awareness. In: *Foundations of Augmented Cognition*. Springer, 656–665.

Hamari, J. et al. (2014) Does gamification work?—A literature review of empirical studies on gamification. In: *2014 47th Hawaii International Conference on System Sciences*, 3025–3034.

Haught, D. and J. Paladino (2012). Improving the reliability and resiliency of the us electric grid. *Metering International*, (1), 46.

Hutchins, E. M. et al. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1, 80.

Kahn, M. N. (2010). *Sentiment market analysis*. FTPress Delivers.

Kaplan, S. and B. J. Garrick. (1981) On the quantitative definition of risk. *Risk analysis*, 1(1), 11–27.

Kaplan, S. M. (2009, Apr.) Electric power transmission: background and policy issues. *US Congressional Research Service*, 14, 4–5.

Kapp, K. M. (2012). *The gamification of learning and instruction: game-based methods and strategies for training and education*. John Wiley & Sons.

Kapp, K. M. (2013). *The gamification of learning and instruction fieldbook: Ideas into practice*. John Wiley & Sons.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Rand Corporation.

Menkes, J. (2009). *Executive intelligence*. Harper Collins.

Naedele, M. (2007). Addressing it security for critical control systems. In: *40th Annual Hawaii International Conference on System Sciences*, 115.

National Research Council. (2010). *Review of the Department of Homeland Security's Approach to Risk Analysis*. The National Academies Press.

NERC. (2010) High-impact, low-frequency event risk to the north american bulk power system. In: *A Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energys November 2009 Workshop*.

Rieber, L. P. (1996) Seriously considering play: Designing interactive learning environments based on the blending of microworlds, simulations, and games. *Educational technology research and development*, 44(2), 43–58.

Stott, A. and C. Neustaedter. (2013) Analysis of gamification in education. *Surrey, BC, Canada*, 8.

Stouffer, K. et al. (2011) Guide to industrial control systems (ics) security. *NIST special Publication*, 800–82.

Vaughan, E. J. and T. Vaughan. (2013). *Fundamentals of risk and insurance*, 11th ed. John Wiley & Sons.

Wolfe, J. (1997) The effectiveness of business games in strategic management course work. *Simulation & Gaming*, 28(4), 360–376.

Wortzel, L. M. (2013). *The dragon extends its reach: Chinese military power goes global*. Potomac Books, Inc.

Zichermann, G. and J. Linder (2010). *Game-based marketing: inspire customer loyalty through rewards, challenges, and contests*. John Wiley & Sons.