CHAPTER 12

CyberCentric: Increasing SME and Citizen Resilience Against Cyberattacks

Babak Akhgar, Jonathan Saunders, Paul Hancock, Alison Lyle, and D. S. Shelton Newsham

12.1 Introduction

CyberCentric[1] is a realistic cybersecurity scenario simulation platform. The objective of *CyberCentric* is to reach out to citizens and small- and medium-sized enterprises (SMEs) to provide them with the capability to share information on cybersecurity-related issues and allow them to experience the impact of cyberattacks as well as learn about means to mitigate against them. *CyberCentric's* overall goal is to provide SMEs and citizens with protective knowledge to improve their cyber resilience. This chapter provides an overview of the game, its developmental concept and key components from a user perspective.

[1] CENTRIC is the Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research at Sheffield Hallam University, UK.

B. Akhgar (✉) · J. Saunders · P. Hancock · A. Lyle
CENTRIC, Sheffield Hallam University, Sheffield, UK
e-mail: b.akhgar@shu.ac.uk

D. S. S. Newsham
Yorkshire & Humber Regional Organised Crime Unit, York, UK

B. Akhgar (ed.), *Serious Games for Enhancing Law Enforcement Agencies*, Security Informatics and Law Enforcement,
https://doi.org/10.1007/978-3-030-29926-2_12

12.2 An Overview of the Cyber Resilience Landscape

The prevalence and related risks of cybercrime are rapidly increasing posing a growing threat to citizens, society, businesses and national critical infrastructure. At the same time, law enforcement agencies (LEAs) grapple with the challenge of keeping pace with developments, including issues such as how best to approach the investigation of such crimes, how to protect the public and businesses against cyberattacks and how to increase society's resilience through better awareness of the threats posed by cyber-related risks. LEAs already offer such advice for more traditional crimes but advice on how to guard against cybercrime is currently less coherent. For example, the UK government provides schemes such as *Cyber Essentials*[2] for SMEs and *Cyber-Streetwise* for citizens,[3] and individual LEAs have their own schemes through regional cybercrime units. In the EU, ENISA promotes cybersecurity in the context of the 'cybersecurity month'.[4]

The education of citizens is paramount, since citizens not only protect and improve their own personal cybersecurity; these are the same people who work in businesses and public organisations, which means their lack of experience in handling cybersecurity increases the potential of vulnerabilities also for their workplaces. Consequently, cybersecurity needs to be tackled from the ground upwards starting with the education of citizens on good preventative practices in the hope that they take this expertise forward into their working environment.

The growing threat of cybercrime has been recognised at the EU level in the European Security Model,[5] which highlights the threat of and the fight against cybercrime as one of the EU's key priorities from 2015 onwards. The European Security Model is defined as being an 'integrated EU security architecture containing common tools for collaboration between law enforcement authorities and judicial bodies within the Member States'.[6]

[2] https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

[3] https://www.cyberstreetwise.com

[4] https://cybersecuritymonth.eu

[5] http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

[6] http://www.focusproject.eu/web/focus/wiki/-/wiki/ESG/European+Security+Model

12.3 Background to the Development of CyberCentric

The development of *CyberCentric* was initiated by observations in an earlier EU-funded project COURAGE[7] that many small- and medium-sized enterprises (SMEs) missed out from the typical cyber-awareness information and events, as these usually focus on larger companies and cities. Especially, the solutions discussed at these events address mostly larger businesses. In consequence, the resilience of SMEs against cyber-based attacks often remains limited. Another factor reducing cyber-preparedness in SMEs are the costs of both attending to and investing into resilience-focused solutions. These gaps lead to the idea of testing the effectiveness of a serious games platform that provides an immersive learning environment, allowing them to experience virtual cyberattacks and learn how these, and subsequent decisions business owners take, may impact their business.

The development of *CyberCentric* was led by a multidisciplinary team of experts formed through funding provided by the High Value Investments and Impact Fellows programme (2017–2018, Sheffield Hallam University, UK). The team consisted of experts in informatics, game design, game development, business resilience and cybersecurity as well as police officers. The game development used the CENTRIC serious games design framework (see Chap. 8) with scenarios developed in cooperation with subject matter experts and police officers.

12.3.1 Iterative Development of CyberCentric *Through a Consecutive Piloting Approach*

The development of *CyberCentric* followed an iterative end-user-based piloting approach (cp. Bayerl & Jacobs, 2017). Pilots in this context refer to preliminary small-scale investigations, which aim to assess the efficacy and feasibility of a product or process (Thabane et al., 2010). Pilot studies are also referred to as *pilot testing* or *pilot experiments* and are a subset of feasibility studies. *Feasibility studies* is an umbrella term, which also includes proof of concept studies. The latter is carried out before the work on a deliverable begins and aims at investigating whether there is an actual need for the proposed game or product. Pilot studies, in contrast, aim to

[7] EU Research COURAGE project. See Akhgar and Brewster (2016).

assess the quality of the product in development as well as the effectiveness of the developmental processes (Eldridge et al., 2016).

Pilot studies gather feedback from end users with the aim to identify areas of the game that work well and areas that end users would like to see improved (Van Teijlingen & Hundley, 2001). Sauro (2018) recommends the use of a combination of expert and novice users. Observing novice users interacting with the system can result in unexpected or unintentional means of interaction with the system (Dix, 2007). Novice end users may thus identify weaknesses that experts or developers may not have acknowledged or identified, as their experience can cause them to overlook fundamental usability issues (Sauer, Seibel, & Rüttinger, 2010). In consequence, a combination of expert and novice feedback will often lead to the most valuable input to improve the game's usability, aesthetic design and efficacy.

Pilot studies are often conducted early during the game development period. Such an early validation can save time and money by solving problems at an initial stage, preventing costly changes at a later stage. Still, even for the first pilot the game should be at a suitable stage to be tested by end users, meaning it has basic functionalities and sufficient features to obtain useful feedback for the further progression of the project. In addition, the game should be thoroughly tested in-house before it is taken to the piloting stage. If the system crashes or unexpected errors occur during the pilot, it may not be impossible to obtain feedback from the participants. To avoid technical issues during pilot testing, a stable build should always be available, whilst any last-minute alterations should go into a separate build. Similarly, if data collection methods have not been well planned, necessary data may not be captured which results in a waste of time and resources (Thabane et al., 2010). Thus, the pilot methodology should be as meticulously prepared as the game design and presentation.

In addition to the first pilot, serious games pilots should be planned in regular intervals throughout the life cycle of a game development project. This long-term focus creates milestones and deadlines to work towards, which ensures that the development does not fall behind schedule, the final product is validated by end users and fits their needs and the development team has not lost sight of the overall aims of the project (Van Teijlingen & Hundley, 2001). Later pilots may have different aims such as making additional improvements on its design and functionalities or may be more narrowly focused on a specific aspect of the game such as the artwork.

Generally, before a pilot study takes place, clear decisions must be taken about:

1. The aims and desired outcomes of the pilot study as a whole and for each iteration
2. The best methodology with respect to data collection methods, analysis of the data, sample size, sample demographics, pilot location, length of the study, etc.

Once the aims of the pilot study are defined, a strategy for the collection of data can be formulated. Defining specific and clearly identifiable outcomes facilitates the evaluation of the game and allows a direct comparison of results across several pilot iterations (see also Chap. 9). Examples for potential outcome measures for serious game pilot studies are:

- How user friendly is the system?
- To what extent do players achieve intended learning outcomes by using the game?
- What are barriers to achieving the intended learning outcomes (skills, behaviours, attitudes, etc.) with this game?
- Is the design of the game appropriate for the targeted user group?
- How long does it take a novice to complete the game or a stage of the game?

The above considerations underpinned also the validation efforts of *CyberCentric*. Using action research as underlying research methodology, the game was validated in five consecutive pilot events, in which participants from local SMEs could experience the serious game and benefit from the attendance of experts for additional information and support. The pilot events were planned and took place in smaller towns across one UK region. Care was taken to create and maintain new and mutually beneficial relationships with police cyber units, with the positive effect that all but one of the pilots were attended by police officers. The lessons learned during each event were fed back to the project team to improve the performance of the game and to fine-tune the scenarios. In addition, briefings and positive information campaigns provided by Europol EC3 (European Cybercrime Centre) enhanced the understanding of the overall risk areas for SMEs. In this refinement phase, the project team considered perfor-

mance aspects from effectiveness of the serious game to user requirements and feedback. The feedback gathered throughout the five pilot events suggests that the game could be used successfully by the diverse group of participants, all of whom gave overall positive feedback about their experience and the value of the game for its intended purpose.

12.4 Concept of CyberCentric

The development of *CyberCentric* brought together experts from LEAs, businesses and academia with the intention to consolidate diverse knowledge about how best to protect businesses and citizens from cyberattacks using a serious game. The concept and content of *CyberCentric* is thus grounded in a wide-ranging and far-reaching exploration of the key factors that support (or threaten) cyber resilience of citizens and SMEs.

The overarching goal of *CyberCentric* is to comprehensively and iteratively address the interrelated facets that underpin protection and mitigation – including the motives, opportunities and networks around cyberattacks, whilst its main focus is to improve the protection and mitigation of cybercrime with a focus on strengthening businesses' cyber resilience and minimising the impact of attacks. In order to achieve this, *CyberCentric* has taken a comprehensive approach that brings together LEAs' knowledge of cybercrimes, the viewpoints of citizens, the actions and reactions of cyber criminals, current policy, strategy and legal governance and combined them with serious game expertise underpinned by an empirically developed design framework (see Chap. 8). The game content is presented as narratives in the form of scenarios around cyberattack and vulnerability issues within SMEs (see Fig. 12.1). The citizen version of *CyberCentric*, focused on SMEs, is freely available to the public. A second version addressing LEAs is intended to reside within the secure network of LEAs for an analysis of resilience issues pertinent to small- and medium-sized businesses.

CyberCentric was created with ease of use and accessibility in mind. To make the game accessible also to users with little to no technical knowledge, the entire system is built on a question and answer system, which requires the user to balance three factors: funds, reputation and resilience. This balancing act enables the game to gamify the resilience building process with actions costing funds but potentially improving or hurting a company's resilience/reputational score (see Fig. 12.2). The gamification approach aims to make the gameplay more attractive and engaging (see Chap. 5).

Fig. 12.1 Introduction page to the game presenting the game's scenarios

12.4.1 Scenarios

Since the cyberthreat landscape changes constantly, *CyberCentric* requires adaptability. The game is therefore split into two facets: The first is the story mode, which introduces users to the main challenges any business could face when trying to remain resilient to cyberattacks; the second presents emerging threats, which can be rapidly added to the game to

Fig. 12.2 Question and answer system

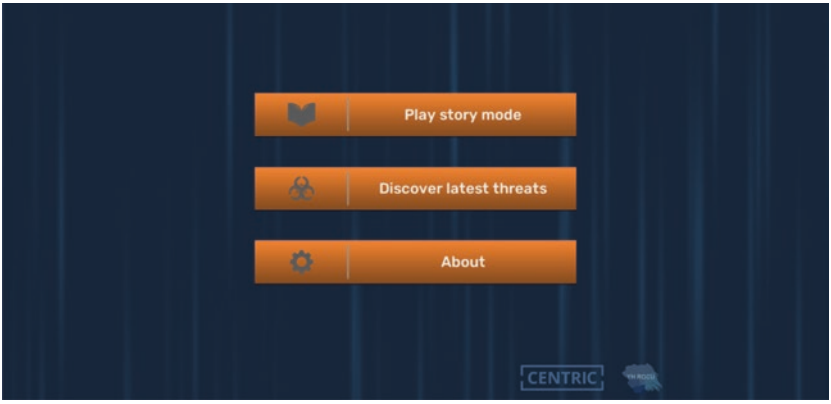

Fig. 12.3 The two facets of *CyberCentric* (main menu)

quickly update methods of responding to and mitigating new cyberattacks (see Fig. 12.3).

CyberCentric currently contains five story narratives. These are: (1) information security, (2) data theft, (3) malware attacks, (4) denial of service and (5) GDPR. Alternative scenarios can be added to the game as soon as new user requirements or new cyberthreats emerge. Through all

scenarios, the user is encouraged and directed towards a better understanding of cyber protection issues. The latter is supported by the inclusion of cyber situational awareness performance elements relevant to SMEs (captured in the indicator's money, reputation and cyber resilience; cp. Fig. 12.2). This ensures that the different scenarios in *CyberCentric* do not appear as disconnected components but rather as a set of interrelated challenges of cyber resilience more generally.

Below, two of the five scenarios are described in more detail to demonstrate the setup of the game environment, how scenarios address the attack vectors used to carry out a specific cyberattack and the expected learning outcomes of the game.

Information Security Scenario: Business Information Security Breach
Scenario: The player's business has experienced a significant data breach, in which hackers have accessed the company's customer databases and stolen personal details as well as credit card information. The attackers have contacted the player's company and are requesting a significant payment for not selling the information on the dark web. The player's business has reviewed the situation and discovered that the hackers gained access by social engineering. The hackers posed as the Chief Information Officer (CIO) of the company requesting remote access rights to the database whilst abroad on holiday. It is believed that the hackers were monitoring the Chief Information Officer and, due to a personal social media profile, discovered that the CIO was on vacation. Upon receiving the email from the supposed CIO, the IT support staff immediately proceeded to update the database access rights as requested, giving the attackers direct access to the databases and all information stored within.

Attack vectors: This scenario presents common attack vectors of information security threats such as unauthorised access to databases through hacking, taking advantage of poor employee cybersecurity, social engineering and insider attacks. This initial approach is then followed up by a ransom request, threatening the public release of documents or the sale of documents online to other criminal organisations.

Expected learning goal – protection: Player should learn the necessity to have checks and policies in place to secure employees against social

engineering methods. They also need to be aware of management decisions that may cause employee dissatisfaction, anger, etc. and consider which access levels individuals (need to) have as well as the level of cybersecurity education of their employees. Prevention measures proposed in *CyberCentric* are, for instance, increasing the awareness of staff about cybersecurity issues, threats and social engineering techniques and maintaining up-to-date cybersecurity policies.

Expected learning goal – mitigation: The player is made aware that each business requires policies that govern how the business must react in the event of a breach, including how to inform all those who need to know such as data protection authorities and the individuals involved. The game also raises awareness that preventative actions should be taken with respect to blocking accounts, updating passwords and additional vigilance in case of potential identity theft. It further advices to involve cyber police specialists at the earliest opportunity and to preserve evidence. Policies should be put in place that demand the validation of information requests and guide the sharing of any secure data or personal access requests.

Malware and Virus Scenario: Botnets

Malware has spawned a field of crime that is cyber-dependent (opposed, for instance, to phishing-based frauds, which are cyber-enabled). Malware, viruses and subsidiaries such as ransomware, keyloggers and adware are common threats faced by typical computer users. These threats are now also making their ways onto mobile and tablet devices.

Scenario: This scenario states that the SME owner has not updated the company's IT software system and that for cost reasons no cyber protection such as a firewall is in place. In consequence, the computers of multiple unwitting victims of malware have been linked to form part of a botnet, i.e. a network of infected computers that can be controlled by the criminal(s).[8]

[8] Botnets can be used to push other strains of malware, harvest users' credentials, compromise their online bank or other accounts, exfiltrate confidential information or facilitate other crimes such as denial of service attacks, spam email campaigns or ransomware attacks. Often botnets can compromise many thousands of computers. For example, *GameOver Zeus* had over 326,000 victims globally (cp. goz.shadowserver.org/stats/), and *Conficker* – a piece of malware known since 2008 – still has over 600,000 infections globally (cp. https://www.

Attack vectors: Malware at scale is typically propagated through mass email campaigns with an attached 'loader' or a hyperlink to malware or through so-called 'watering-hole' attacks where websites are compromised and systems of visiting users with unpatched or vulnerable systems become infected. This scenario presents common attack vectors for collecting personal and business information via a malware-based infection of the company's IT system.

Expected learning goal – protection: CyberCentric raises awareness of protective measures from technical solutions, which can block many of the malicious infection vectors, to proper Internet hygiene. The latter means that users are educated into maintaining healthy, patched operating systems with updated antivirus software and further avoid risky situations such as opening unsolicited emails and/or clicking on links. *CyberCentric* improves users' understanding of how malware-based attacks are propagated and why employees may not maintain or implement the security measures that are available.

Expected learning goal – mitigation: CyberCentric supports citizens and LEAs by:

- Educating businesses on the identification of infections and infection vectors and on the best courses of action, for instance, in the UK contacting hubs such as Action Fraud and NCA
- Seeking ways to clearly outline indicators of compromise and vendor name confusion to assist in the earliest possible identification of a malware threat
- Providing clear guidance for victims and investigators on how to prevent further losses and victimisation, how to identify and quantify losses and where clean-up tools/solutions may be found

grahamcluley.com/2015/12/seven-years-conficker-worm-dead-dominating/; http://www.shadowserver.org/wiki /pmwiki.php/Stats/Conficker). Crime of this scale requires a paradigm shift in approach for law enforcement globally.

12.5 Expected Outcomes for SMEs and Citizen's Perceptions and Behaviours

CyberCentric has an explicit focus on changing the perceptions and behaviours of citizens and SMEs with respect to cyberthreats through story boarding and up-to-date information on the latest cyberthreats. Despite repeated efforts, SMEs are often not as aware of cybercrime threats as they should be – or they do not behave according to the knowledge they have. This is borne out by results from the Eurobarometer Cybersecurity Survey,[9] which was carried out in 2013, 2014 and 2015 employing surveys and interviews combined with additional background research. According to this survey, only half of EU citizens felt well informed about the risks posed by cybercrime despite the fact that over one million people are victims of cybercrime every day. In particular, the Eurobarometer findings suggest that citizens are increasingly concerned about the misuse of personal data and the security of online payments, the prevalence of identity theft, malicious software, banking/credit card fraud, social/email account hacking, scam emails and general online fraud, linked with a declining level of trust in those who hold personal data including public authorities.

CyberCentric seeks to empower citizens and SMEs to understand and perceive the risks of cybercrime and its threat for themselves and their business processes. Identifying these gaps in citizens' knowledge and how they perceive cybersecurity enables the development of strategies to facilitate awareness and tools for taking preventative actions. With the help of *CyberCentric*, SMEs and citizens receive capabilities to:

- Develop a knowledge base that helps to build an accurate understanding of risks, threats and impacts of cybercrime on their daily business processes
- Explore the conflicts and contradictions in maintaining the balance between privacy and security, its applicability to cybercrime, its relevance to businesses and its impact on policy and data protection guidelines
- Inform citizens about the most critical vulnerabilities and privacy issues and adapt this information to a number of different groups (e.g. young people, elderly, those lacking technical knowledge, etc.)

[9] http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2019

- Identify the role and rationale behind the current security behaviours of citizens and the opportunities these behaviours create for criminals and in consequence to develop techniques to raise awareness and incentivise the implementation of better, more effective preventative actions taking into account the failures and gaps in existing awareness-raising campaigns

12.6 Conclusion

CyberCentric addresses the rising threat of cyberattacks for citizens and business, putting a special emphasis on small- and medium-sized enterprises that often lack the knowledge or resources to harness large-scale cyber defences. The objectives of the game are to raise awareness of cyberthreats as well as to improve cyber-related knowledge on how to prevent and mitigate against such attacks. Instead of promoting large-scale investments, which may be unrealistic for citizens and SMEs, the focus lays on often simple, but effective means from employee training to the creation of data management policies. The current scenarios focus on five prominent threats, although the modular design of *CyberCentric* makes it easy to develop additional scenarios as new threats emerge or to modify existing scenarios to reflect technological or legal changes. The game has been translated into Croatian, demonstrating that the concept and content is transferable across national boundaries and communities. Overall, experiences from end users suggest that *CyberCentric* offers a meaningful approach to enhance cyber resilience for citizens and businesses. It can serve as a positive example for law enforcement agencies aiming to engage with the public and local businesses on how to better prevent modern forms of crime.

References

Akhgar, B., & Brewster, B. (Eds.). (2016). *Combating cyber cime and cyber terrorism*. Cham, Switzerland: Springer.

Bayerl, P. S., & Jacobs, G. (2017). Evaluating the design and implementation of CP-support technologies: A participatory framework. In P. S. Bayerl, R. Karlovic, B. Akhgar, & G. Markarian (Eds.), *Community policing - A European perspective* (Advanced sciences and technologies for security applications) (pp. 247–267). Cham, Germany: Springer.

Dix, A. (2007). *Designing for appropriation*. Proceedings of the 21st British HCI Group Annual Conference on People and Computers (pp. 27–30).

Eldridge, S., Lancaster, G., Campbell, M., Thabane, L., Hopewell, S., Coleman, C., et al. (2016). Defining feasibility and pilot studies in preparation for randomised controlled trials: Development of a conceptual framework. *PloS one, 11*(3), e0150205.

Sauer, J., Seibel, K., & Rüttinger, B. (2010). The influence of user expertise and prototype fidelity in usability tests. *Applied Ergonomics, 41*(1), 130–140.

Sauro, J. (2018). *Do novices or experts uncover more usability issues?* Available online: https://measuringu.com/novice-expert-issues/

Thabane, L., Ma, J., Chu, R., Cheng, J., Ismaila, A., Rios, L., et al. (2010). A tutorial on pilot studies: The what, why and how. *BMC Medical Research Methodology, 10*(1), 1–10.

Van Teijlingen, E., & Hundley, V. (2001). *The importance of pilot studies.* Social Research Updates, 35. Available online: http://sru.soc.surrey.ac.uk/SRU35.pdf