Title: CyberGaTE: A Gamified Virtual Training Environment for Cyber-Security

Abstract: The findings of the latest cyber security status report by ISACA indicates shortage of cyber-security professionals is universal and ongoing. A further study conducted by the Ministry of Universities and Science has identified a skills gap that exists amongst the fresh cyber-security graduates, who often do not possess the ability to apply their skills to real-world scenarios as employers demand. The study further identifies that the businesses value experience more than academic qualifications.

Effective cyber-security education unlike most other technical subjects not only requires a hands-on, real-world learning environment but also demands a change of behavior amongst the learners.

CyberGaTE, HEA funded project aims to bridge the skill-gap between theory and practice as well as address the specific needs of effective cyber-security training through innovative pedagogical practices such as gamification and challenge-based learning.

Gamification is defined as applying game mechanics in a non-gaming context. Game players regularly exhibit persistence, risk-taking, attention to detail and problem solving; all behaviors are ideally suited for effective cyber-security training . Some gaming techniques that shall be explored are real-life problem-based storytelling that would form the basis of the learning content and the use of characters (avatar/role play) and the use of narrative to create a bond between the learner and the avatar thereby enhancing engagement as suggested by literature.

The objective of CyberGaTE is to develop a holistic cyber-security training that enables the change in learner's behavior by making them security conscious for every action they perform in the real-world environment. This would be achieved by hosting the gamified learning resources on a virtual training environment using the innovative concept of 'Classroom as a Service', offering the required hands-on real-world experience. The project aims to engage employers and students to build and assess CyberGaTE's effectiveness as well as disseminate good practice in industry and academia.

References

[1] ISACA (2015), 'Global Cybersecurity Status Report', [Available Online] http://www.isaca.org/pages/cybersecurity-global-status-report.aspx as accessed on 12th October 2015

[2] H M Government (2014), 'Cyber Security Skills - Business perspectives and Government's next steps', [Available Online] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf as accessed on 12th October 2015

[3] Bada, M., Sasse, A., & Nurse, J. R. (2014). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. Report). Global Cyber Security Centre.

[4] Klopfer, E., Osterweil, S., & Salen, K. (2009). Moving learning games forward.

[5] Adams, M., & Makramalla, M. (2015). Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. Technology Innovation Management Review, 5(1).

Dr Chitra Balakrishna
Senior Lecturer in Computing
Edge Hill University

Prof Daniela Romano
Professor of Computing
Edge Hill University

James Coleman
Senior Lecturer in Computing
Edge Hill University