SUCCEED Approach for Better Cyber Security and Counter Terrorism Education

Budi Arief, Tom Anderson
School of Computing Science
Newcastle University
Newcastle upon Tyne, UK
{budi.rief, tom.anderson}@ncl.ac.uk

Rosie Borup, Louise Rutherford
FoCES / Creative Communities Unit
Staffordshire University
Stoke-on-Trent, UK
{r.borup, louise.rutherford}@staffs.ac.uk

Abstract—This paper introduces the SUCCEED project, which aims to help tackle issues related to cyber security and terrorism through education and partnership. By sharing the project outcomes with target groups – such as higher education institutions, critical infrastructure organisations, government agencies, relevant public and private sector companies – we hope to ensure that future university graduates are able to contribute positively to the cyber security and/or counter terrorism strategy of their place of work. In this paper we present some preliminary results from the project; these results were obtained from several workshops that we conducted, taking input from representatives from industry, government organisations, and education initiatives. Our work is ongoing, and we welcome feedback and potential collaboration to improve our collective efforts towards designing and implementing new or improved products and services aimed at the prevention, detection or response to cyber threats and terrorism activities.

Keywords—education; curriculum development; cyber security; counter terrorism; industry engagement

I. INTRODUCTION

The threat of physical or cyber-attack targeting major infrastructure is a growing concern in our society. The “taken for granted” security of various infrastructure systems has evolved into a new area, Critical Infrastructure (CI), as a result of the 9/11 attacks in the USA [3]. CI refers to the systems, processes and mechanisms which support the delivery of essential services such as the supply of water, electricity and gas; schools and hospitals; roads, railways and airports; telephone and the Internet; information and communication; banking and finance; emergency services; sewage and refuse disposal, and so forth. While individual infrastructure systems provide unique services, it is also important to consider the interdependency of various infrastructures, since the failure of one could lead to the collapse of others, with the potential to close down a whole range of crucial services. For example, a physical attack on an electricity grid could lead to the failure of a number of other services such as hospitals, railways and airports. Recent Stuxnet [2] and Sony Pictures [1] incidents emphasise the high stakes involved in cyber security, with the possibility of cyber incidents affecting national security and causing diplomatic fallout.

There are many ways in which Critical Infrastructure Protection and Security (CIPS) can be addressed, and a major opportunity is through better education. Indeed, as educators of future employees in all areas of CI, universities have an obligation to include cyber security and terrorism awareness as part of their preparation of students for their working life. In order to do this effectively, it is vital that universities liaise with key employers and listen to their needs. Only when these needs are understood can universities contribute effectively to prepare students for their place in these organisations. This is the main driver behind the SUCCEED (Shaping University Curricula to Critical Infrastructure Employer Needs) project (http://www.succeed.eu.uk/) presented in this paper.

The SUCCEED project is simple in concept, but high on potential impact. By ensuring that there is a thorough understanding of how Higher Education Institutions (HEIs) can contribute, based on research and consultation with key employers, HE curricula can be developed in a planned, strategic manner, leading to a cross-faculty, coherent CIPS delivery capability across all undergraduate and postgraduate programmes. Another important outcome of the project will be to inform stakeholder groups, such as research teams, to help direct efforts towards the design and development of new or improved products and services aimed at the prevention, detection or response to criminal and terrorist activities.

The rest of the paper is organised as follows. Section II outlines the SUCCEED work plan, while Section III provides a summary of what we have learned so far, mostly from the workshops completed to date. Section IV concludes our paper and outlines the work that still needs to be done.

II. SUCCEED WORK PLAN

The SUCCEED project commenced in September 2014, and it is scheduled to run for 18 months. The partners involved are Staffordshire University (coordinator) and Newcastle University. This consortium brings together expertise in complementary areas of counter terrorism (Staffordshire) and cyber security (Newcastle).

Four main stages of work have been planned:

1. Ask relevant employers to tell us what, and how, universities can contribute towards both the prevention of, and preparedness for, acts of cybercrime and terrorism, with regard to providing guidance for the future workforce (represented as the “Ask Employers” and “Needs Analysis” tasks shown in red in Fig. 1).
2. Carry out a university-wide, cross-discipline curriculum investigation and mapping exercise to find out what is already taking place and what is missing (“Gap Analysis” – shown in green in Fig. 1).
3. Improve the ways universities support organisations to protect people, property and data, based on the evidence and lessons gathered from our research (“Recommendations” – shown in blue in Fig. 1).
4. Test our ideas against real-world expertise through consultation and dissemination to maximise impact (“Ask Employers” and “Disseminate and Exploit” tasks shown in purple in Fig. 1).

Currently, we are at the stage where the first Ask Employers task has been completed (it was performed through a series of workshops involving participants from several employer sectors). We are now in the process of carrying out a full Needs Analysis utilising the data that was obtained.

III. PROGRESS SO FAR

We present here the preliminary findings from the first three workshops (the fourth was held in May 2015, so we have not yet analysed the data from this workshop). More details can be found at [http://www.succeed-eu.uk/project-results](http://www.succeed-eu.uk/project-results).

**TABLE I. SECTORS REPRESENTED IN THE FIRST THREE WORKSHOPS**

<table>
<thead>
<tr>
<th>Workshop 1</th>
<th>Workshop 2</th>
<th>Workshop 3</th>
</tr>
</thead>
</table>

The workshops were run by a facilitator, posing several key questions (such as “What is your background”, “What are the issues of concern of your organisation”, “What would your organisation do in a particular scenario”, and “Where are the gaps in your organisation”) that were answered in a small groups exercise involving all participants. Participants came from diverse yet complementary sectors, as listed in Table I.

To understand the “needs” factor, we looked at the cyber security and terrorism concerns that participants believe could affect their organisation. Results from the first three workshops are summarised in Fig. 2. There are several themes emerging (e.g. the importance of staff training, the need for a “security culture”, and the growing importance of data security). Other preliminary findings are shown in Table II.

We still need to carry out a more detailed analysis on the combined data from all four workshops to be able to extract a more accurate picture. This work is ongoing, and we will share the results in due course.

**TABLE II. OTHER PRELIMINARY FINDINGS FROM THE WORKSHOPS**

<table>
<thead>
<tr>
<th>Gaps Identified so far</th>
<th>The Perfect Organisation ...</th>
<th>The Perfect Employee ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Staff training</td>
<td>• Has an open, collective, supportive culture</td>
<td>• Demonstrates integrity</td>
</tr>
<tr>
<td>• Commitment to</td>
<td>• Is risk aware</td>
<td>• Has appropriate technical skills</td>
</tr>
<tr>
<td>investment</td>
<td>• Encourages open and honest behaviour</td>
<td>• Possesses relevant, up-to-date knowledge</td>
</tr>
<tr>
<td>• Clear, effective policy on BYOD</td>
<td>• Commits to being a “learning” organisation</td>
<td>• Communicates well and is able to influence others</td>
</tr>
<tr>
<td>• Policy for flexible working practices</td>
<td>• Communicates standards clearly</td>
<td>• Has customer focus</td>
</tr>
<tr>
<td>• Code of ethics</td>
<td>• Ensures standards are upheld by all</td>
<td>• Shows a positive, open attitude</td>
</tr>
<tr>
<td>• Awareness during recruitment</td>
<td>• Adequately resourced</td>
<td></td>
</tr>
<tr>
<td>• Employment contract terms</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**REFERENCES**

