HOW TO SUCCEED IN CYBERSPACE

T Anderson[1], B Arief[1], TN Basit[2], R Borup[2], L Rutherford[2]

[1]Newcastle University (UK)
tom.anderson@ncl.ac.uk, budi.arief@ncl.ac.uk

[2]Staffordshire University (UK)
t.n.basit@staffs.ac.uk, r.borup@staffs.ac.uk, louise.rutherford@staffs.ac.uk

Abstract

Cyberspace is a very real man-made environment. Like any physical realm, while it offers potential for progress and benefits, it also offers opportunities for misconduct, and cyber criminals and cyber terrorists are continually searching out weaknesses in the defences that have been erected against them. There is one weakness that is pervasive across society: our individual lack of awareness, and of how to protect ourselves and our organisations against cyber attack. This paper reports on an EU funded project called SUCCEED (Shaping University Curricula to Critical Infrastructure Employer Needs) which seeks to reduce that vulnerability through education; specifically, we want to advise Higher Education Institutions of measures by which curricula can be augmented to ensure that all graduates have an appropriate level of cyber savvy. The paper's structure reflects the project's straightforward approach: first we identified what is needed in terms of knowledge and understanding of how to be protected in cyberspace; second we examined current provision (primarily to identify gaps, but also to refer to best-practice); third we will outline recommendations based on our findings from the first and second phases; and fourth we will have these recommendations validated by relevant stakeholders (including representatives from industry, government organisations and academia) in order to distil our conclusions, which will be disseminated and exploited further as final contributions of the project. This paper presents current progress of the SUCCEED project, in particular the results and findings obtained from the first two phases of the project. This is a relatively modest project, and will not claim to provide a definitive solution. However, we believe it can provide an important first step towards an enrichment of curricula that will better prepare graduates to cope with the dangers and risks from terrorists and cyber criminals in the digital future they will all participate in. Only thus can they SUCCEED in cyberspace, by staying safe and secure in the digital realm – through *education*.

Keywords: cyber, higher education, digital security, terrorism, cybercrime

1 INTRODUCTION

Cyberspace is a very real man-made environment, supported by colossal investment in digital resources. Unfortunately, that cyber reality – like the physical realm – provides manifold opportunities for misconduct, ranging from relatively petty theft to massive fraud, from dubious pornography to facilitating sexual offence against children, from overwriting a website to disrupting critical national infrastructure.

As well as providing immense benefits to society (and these benefits continue to grow, year after year) the exponential increases in computing power (in terms of speed and storage, as well as of networked interconnections [1]) also give new avenues for malicious acts to criminals and terrorists [2]. These cyber criminals and cyber terrorists are continually searching out weaknesses in the defences that have been erected against them, such as encryption, firewalls and passwords, but there is one weakness that is pervasive across society: our individual lack of awareness, and of how to protect ourselves and our organisations against cyber attack.

The threat of physical or cyber attack targeting major infrastructure is indeed a key concern globally. Vulnerability to sudden service disruptions due to deliberate sabotage and terrorist attack is a major threat [3]. The "taken for granted" security of various infrastructure systems has evolved into a new discipline, Critical Infrastructure Protection, as a result of the 9/11 attacks in the USA [4]. This is even more pertinent now, given the subsequent terrorist attacks that have occurred throughout the world over the last decade. Critical infrastructure comprises goods and services such as clean air; the

supply of water, electricity and gas; schools and hospitals; roads and bridges; railways and airports; telephone and the Internet; information and communication; banking and finance; emergency services; sewage and refuse disposal, and many others. The concept of critical infrastructure protection and security is associated with the capability to defend against – and capacity and readiness to respond to – serious incidents encompassing the critical infrastructure of a nation or region; infrastructure that is crucial for the wellbeing and safety of nation states.

While individual infrastructure systems provide unique services, it is important to consider the interdependencies between infrastructures, because the failure of one could lead to the collapse of many others, with the potential to close down multiple crucial services. For example, a physical attack on an electricity grid can lead to the failure of a number of other services such as in hospitals, railways and airports. Similarly, a cyber attack on telecommunication networks could have a deleterious impact on police and emergency services.

Thus *critical infrastructure* denotes a wide array of resources that are necessary for the functioning of social, economic, political and cultural systems of a nation [5]. Due to the scale and complexity of the critical infrastructure required to operate in contemporary society, such infrastructures are vulnerable to both physical and cyber threats [6]. It is clear, and widely acknowledged, that a disruption to such resources can cause loss of life, damage to property, and substantial economic costs. While the threat is very real, the prevention and protection of critical assets is often only viewed as the responsibility of governments, and little emphasis is placed on educating our citizens to identify, report, and deal with actual or potential physical or cyber security risks. Nevertheless, education and training have a clear role in helping to detect and prevent threats to critical infrastructure and thus avert (or mitigate) later catastrophes.

The wide-ranging use and scope of information and communication technology today makes critical infrastructure vulnerable to cyber as well as physical attacks. Even infrastructure not considered as under threat, such as domain names, can pose security risks [7]. Lewis et al. [8] note that the European Commission (EU) has initiated a network comprising research and technology organisations within the EU with expertise in critical infrastructure, starting with preparatory studies in 2009-2010. They go on to explain the extent of work that has been carried out so far in this area. Focusing on the US context, Biringer et al. [9] contend that strategies to reduce risks relating to Critical Infrastructure Protection and Security (CIPS) conventionally focus on minimising the likelihood of undesirable events by improving the effectiveness of security and protection to mitigate vulnerabilities. They nevertheless argue that it is not possible to prevent all undesirable events, and resilient systems should be designed to ensure swift recovery of critical infrastructure.

In August 2014, the UK national threat level was raised from ‘substantial’ to ‘severe’, signifying that terrorist activity is considered ‘highly likely’ in the UK. British citizens and businesses have been warned to be ‘vigilant’. It is important that individuals and companies be educated to learn to deal with threats to personal and organisational security. Evidently, universities have a role to play in helping businesses and government agencies to protect their people, property and data systems.

This paper presents a report on an EU funded project called SUCCEED (Shaping University Curricula to Critical Infrastructure Employer Needs – http://www.succeed-eu.uk/). The SUCCEED project seeks to reduce by means of better education the current societal vulnerability resulting from a lack of awareness of cyber threats and terrorism; specifically, we want to advise Higher Education Institutions (HEIs) of measures by which curricula in all disciplines can be augmented to ensure that all graduates have an appropriate level of cyber savvy. By ensuring that there is a thorough understanding of how HEIs can contribute (based on research and consultation with key employers), HE curricula can be developed in a planned, strategic manner, ideally leading to a cross-faculty, coherent delivery capability across all undergraduate and postgraduate programmes. When it is germane, we will report more generally on opportunities for specialist training, specific technology needs, or for appropriate further research.

The rest of the paper is structured as follows. In the next section we give an overview of the SUCCEED project, summarising the four planned phases (of which the first two are now almost complete), and the methodology that those phases have adopted. Section 3 presents our results to date, which are largely complete for the first phase, and constitute our interim findings from phase 2. The final section gives a preliminary recommendation and sketches the opportunities for further work.

2 THE SUCCEED PROJECT

The SUCCEED project 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 HEIs, critical infrastructure organisations, government agencies, relevant public and private sector companies – the project hopes to ensure that future university graduates are able to contribute positively to the cyber security and/or counter terrorism strategies of their place of work.

To achieve this aim, four main phases of work have been defined:

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 (**Needs**).
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 (**Gaps**).
3. Improve the ways universities support organisations to protect people, property and data, through a set of recommendations based on the evidence gathered and lessons learned from our research (**Recommendations**).
4. Validate our recommendations against real-world expertise through consultation and dissemination to maximise impact (**Validation, Dissemination and Exploitation**)

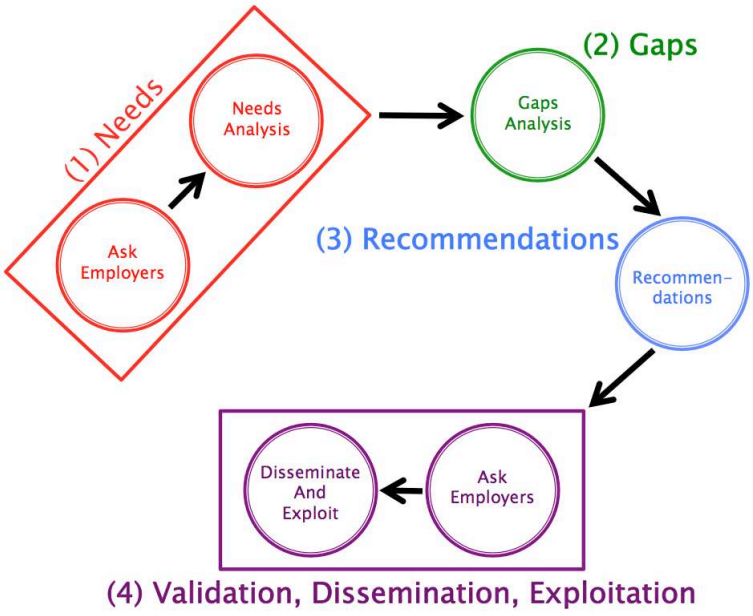

Figure 1. The main phases of the SUCCEED project

Fig. 1 provides a diagrammatical representation of the main phases of the work planned in the SUCCEED project, which will be described in more detail in Section 2.1. At the time of writing, the first two phases of the project (Needs and Gaps) have been largely completed, hence this paper will give a detailed report on these phases, while outlining how the other two phases will be conducted in our future work.

There are three main research questions that the SUCCEED project seeks to address:

RQ 1. What issues are businesses and government agencies concerned with regarding the protection of their people, property and data systems?

RQ 2. How can companies and agencies improve the way they prepare, prevent and manage the consequences of internal and external threats to security?

RQ 3. How can Universities contribute to the security of different organisations through education, research, or development of new products and services?

These research questions drive the approach and methodology taken in the project, which will be described in detail in Section 2.2 below.

2.1 Four Phases of the SUCCEED Project

2.1.1 Needs

In our first phase we held four workshops involving employers from a range of commercial and public sectors. Group exercises involving a number of challenging scenarios were used to extract key areas of concern and priorities from the participants, and we analysed the results to create a weighted enumeration of what were regarded as the most significant issues. To gain added benefit we also sought to summarise what were perceived as common organisational weaknesses and desiderata (for the company and the individual).

2.1.2 Gaps

We conducted a large number of interviews within our own two universities, talking to programme managers, curriculum developers and course presenters. Our overall aim was to ascertain to what extent currently taught material ensured that graduates (in many specific disciplines):

- were aware of the threats and risks that cybercrime and terrorism pose;
- had appropriate knowledge to protect themselves and their organisations;
- acquired relevant skills sufficient to safeguard themselves (and others).

These discussions were held in the light of our findings from the first phase. We noted current good practice, and discussed apparent gaps with our interviewees.

2.1.3 Recommendations

Based on the findings gathered from the Needs and Gaps phases, a set of recommendations will be compiled with an aim to improve ways universities can support organisations to protect people, property and data. In particular, it is envisaged that new teaching approaches will be explored, for example by integrating key cyber security skills into university teaching across all disciplines in a holistic manner.

2.1.4 Validation, Dissemination and Exploitation

Our final phase is to return to the stakeholders: to the employers we consulted initially and to the educators that we interviewed. Feedback on our findings and preliminary recommendations will be used to correct any errors or omissions and to refine the conclusions. We are using digital media and other routes to disseminate these preliminary outcomes so that feedback is also available from the wider community (e.g. delegates to this conference).

2.2 Methodology

Phase 1 of the project was constructed around workshops with stakeholders in business and industry, with an emphasis on critical infrastructure. Data on issues and opinions was extracted from these workshops in a manner akin to voting – an issue raised by a delegate (on a yellow slip) thereby gained a “vote” which other delegates could subsequently increment. Phase 2 was based on interviews with staff at the two universities, in which all interviews followed a structure dictated by a standard questionnaire. Data from the interviews was generated using an online questionnaire response form plus reports from the interviewers. On completion of phase 2 and its data analysis we will formulate a small set of key recommendations and test these out with our business stakeholders and academics, before wider dissemination takes place.

2.2.1 Workshops

Four workshops were organised during December 2014, February 2015, March 2015, and May 2015, mainly to fulfill the first phase (Needs) of the project. At the same time, these workshops also provided insights into the issues relevant to the second phase (Gaps) of the project. The title of the workshops was: “Security: It’s Everyone’s Business”. Two workshops took place at Staffordshire University and the other two at Newcastle University. The first three workshops followed a similar format. The main objective of these workshops was to gather the perceptions of industry representatives on what they

saw as the key cyber and terrorism concerns and threats for organisations in general and critical infrastructure in particular. Workshop participants were also asked to focus on graduates' awareness, understanding and skills required to deal with security, cybercrime, critical infrastructure and terrorism. The fourth workshop was organised in a different way to identify resources that already exist to deal with cybercrime and terrorism. These included the products, services, curriculum, qualifications and training available for this purpose.

Delegates from Banking, Defence, Education, Health, Information Technology, Insurance, Management Consultancy, Police, Security Companies, Telecommunications, Transport, and Utilities sectors were represented at these workshops.

Each workshop used a similar approach to elicit views from participants. Working in groups (set up to maximise diversity) the delegates were asked to discuss case studies and scenarios, and note down the security concerns they thought were relevant for their own organisations. All delegates then had an opportunity to consider the full set of issues identified, and add their own marker where applicable. Lastly, with strict confidentiality assured, delegates were asked to nominate significant gaps in protection from cyber and terrorist threats.

The results obtained from the workshops are presented in Section 3.

2.2.2 Interviews/Questionnaires

In order to gauge the extent of university teaching that addresses cyber security and/or counter terrorism that is currently in place, we have carried out a university-wide, cross-faculty curriculum investigation and mapping exercise at both Staffordshire and Newcastle Universities. This exercise was conducted through a series of interviews involving directors of learning and teaching, programme managers, lecturing staff, as well as other university staff who have an interest in, and influence on, teaching.

Our approach here was again straightforward. Starting from the project's research questions (RQs), we created a small set of RQs specifically for the gaps analysis, and these were refined to give us the questions that were posed to our academic colleagues – in sum these questions were set to elicit information on the presence or absence of taught material relating to the threats and risks posed by cybercrime and terrorism. A first, and necessary, step was to obtain authorisation to go ahead from university management; no difficulties were encountered, Next, rather than simply present a bald questionnaire, we prepared a motivational preamble, and then solicited interviews with a targetted selection of university staff, covering the range of Schools and Faculties at both locations. We offered a 30 minute, structured interview session to go through our short questionnaire, with oral responses that could be discussed and clarified, and then requested submission of an online form so that the interviewees could send in their own considered responses, in their own words. Nevertheless, we retained notes taken at the interview, and wrote up interviewers' reports on these sessions, in order to preserve our own recollections of points made.

2.2.3 Data collection and analysis

The online submission route gives us a set of primary responses from a wide cross-section of academics covering both universities. These responses can be augmented (where appropriate and important) from our own reports – which although technically secondary we do not consider as inferior data. As project participants we may introduce some limited degree of bias, but against this we have a much clearer overall picture in which to embed the information we are given. Initial results from these responses, and the reports, are given in Section 3, next.

Analysis to date has remained subjective; this is appropriate given that there are still a small number of interviews to be conducted (to take pragmatic account of diary scheduling difficulties over the hectic summer period). Indeed, we anticipate that most conclusions will remain subjective, although when the response data set is complete we will, of course, perform a quantitative analysis to extract any reinforcing numerical measurements.

3 RESULTS

In Section 3.1 we give a distillation of the results of our workshops on Needs Analysis (phase 1); this work is essentially complete. Section 3.2 provides a first statement of the outcomes from the Gaps analysis; since our interview programme (phase 2) is not fully completed these may be augmented

later, but we have added to this section the views of our commercial/business stakeholders on Gaps, as expressed at the workshops.

3.1 Needs Analysis

The workshops have given us valuable insights into security concerns faced by organisations (more precisely, from the sectors enumerated in Section 2.2.1). We compiled the findings from the first three workshops and distilled them into nine themes:

1. **Lack of awareness/knowledge/skills**: There was considerable recognition that many people are not fully aware of the risks of cybercrime and terrorism, and that there is a significant shortfall in knowledge and skills for dealing with these threats. This was seen as a current problem, but likely also to be the case for future graduates.
2. **Emerging trends and challenges**: One of the most challenging themes identified concerns the rate and intensity of change in the ways security attacks are being made. But in addition, there are many – and major – areas of current concern, often due to technology advances and consequent changes to ways of working.
3. **Threats and risks**: There are many ways in which someone with malicious intent can threaten a system, a business, users and society at large. The forms taken by these threats are often referred to as *attack vectors* (the route and method of attack). Concern clearly attaches to the risks associated with these attacks.
4. **Data protection**: A major specific concern is the protection of data from unauthorised access, in order to maintain confidentiality, to protect the value of the data, to prevent misuse of the data, to ensure the data is not maliciously modified or deleted, and to prevent the insertion of invalid data, inappropriate content, or malware.
5. **Security culture and clash**: When we consider safety issues, the importance of a 'safety culture' is readily accepted. The prevalence of security breaches impacting on everyday life should lead to a similar recognition of the need for a pervasive 'security culture' which treats protection from digital attack and terrorism as a fundamental need.
6. **Human related issues**: Although almost all security concerns have their origin in decisions by people, the issues in this theme were seen as being immediately and directly related to human factors.
7. **Financial strategy relating to the costs of security**: Costs are incurred to augment security and – especially for commercial enterprises – these costs are an obvious deterrent. Management has to make a difficult strategic decision on cost/benefit where estimates are very uncertain and resources may be strictly limited.
8. **Impact and consequences**: As well as all of the concern for preventing security breaches, it is also necessary to consider the range of deleterious consequences, from loss of life and injury, environmental impact, financial losses, degradations of business and society.
9. **Policies and compliance**: Growing concern by customers is leading to an increased need for compliance with a range of security standards and policy requirements.

Of these themes, lack of awareness/knowledge/skills was deemed to be the most important, as indicated by the count of votes given by the participants of the workshops to the concerns raised (grouped subsequently into the nine themes above). The data count for each of the nine themes is presented in Table 1, while Fig. 2 provides a diagrammatic illustration of the same data expressed in percentage terms.

Table 1. The nine themes of organisations' concerns on security and related challenges

Key Themes	Count
Lack of awareness/knowledge/skills	82
Emerging trends and challenges	75
Threats and risks	68
Data protection	53
Security culture and clash	36

Human related issues	29
Financial strategy relating to the costs of security	18
Impact and consequences	15
Policies and compliance	13

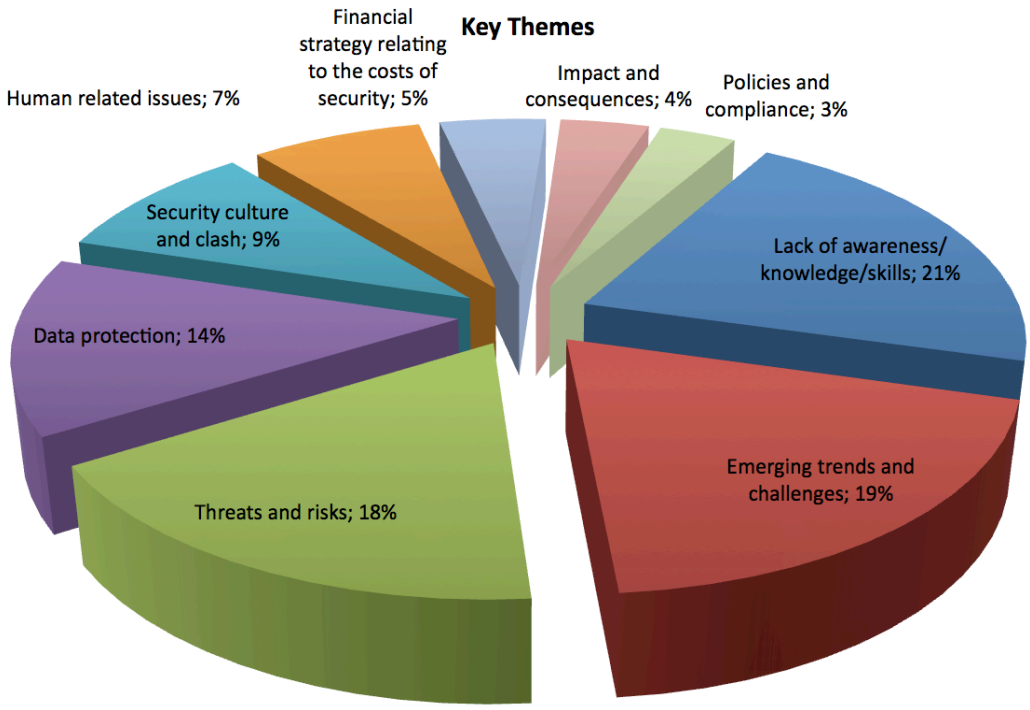

Figure 2. The distribution of the key themes

The workshops have also revealed potential measures to address these concerns, which can be grouped into:

- *education* (count = 37) including training more people in IT skills, prevention by educating students about threats, and prevention by educating staff on how to look for and identify suspicious behaviour
- *awareness* (18) including awareness of operational security issues, and spreading the message not just to the obvious stakeholders, but to everyone engaged with the organisation
- *system* (15) including resilience of ICT systems and infrastructure
- *physical* (11) including physical security of buildings and computers, as well as access controls

Fig. 3 depicts what delegates at the SUCCEED workshops believed to be the most appropriate measures in tackling cyber security and terrorism challenges.

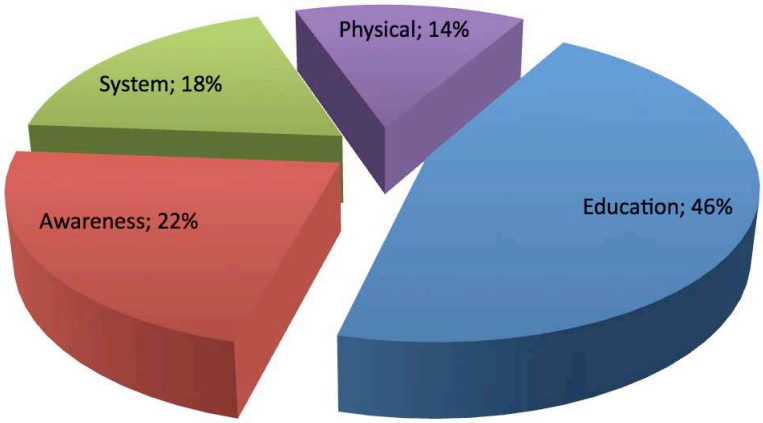

Figure 3. The distribution of potential measures to address the challenges

3.2 Gaps Analysis

3.2.1 Findings from workshops

In the first three workshops, the delegates were also asked to undertake an analysis of where gaps might occur in their organisations' practice with regard to prevention, preparedness and consequence management, as well as to list gaps that currently exist in dealing with the scenarios that they had been presented with. These activities resulted in the identification of three main types of gaps:

- Gaps in **Society**: mostly related to *awareness* (people who do not think that the threats are relevant to them – "it happens to someone else"), and *understanding* (people who are not aware of the risks in the digital era, where they have open access to smart phones, tablets and the like)
- Gaps in **Business/Organisations**: dividing line between converts who are making a generational or paradigm shift and those focused on profitability and commerce who don't really care; entrepreneurs wanting only to "rake money in" – they breach security systems and collect personal data for commercial exploitation (no ethics); and lack of employees' understanding of responsibility for security, i.e. lack of security culture
- Gaps in **Government**: not addressing the need to create a security culture

The delegates were also asked to suggest potential ways to plug these gaps and who should be responsible to implement these, as summarised in Table 2.

Table 2. Addressing the gaps in security and counter terrorism provision

Who	How
Higher Education Institutions	• Undergraduate and postgraduate teaching, including teaching dynamic risk analysis (a model to assess risk which is constantly evolving), raise awareness of digital space and responsibility for own digital footprint and employers' requirements, and include security within teacher/lecturer training • Resources – produce a Sustainability Framework, including doorways for introducing security themes, a methodology for adopting and embedding a security culture, and dynamic risk analysis • Consultancy – provide for organisations, based on the premise: Threat + Vulnerability = Risk • Curriculum development: embed principles of cyber security and anti-terrorism within all courses, research jobs of the future, map out the IT skills gap and develop material to fill the gap, and develop relevant degree programme • Applied research: such as security for big data and psychology behind cybercrime and terrorism • Provide academic staff to employers for supervision/mentoring • Encourage a multi- and inter-disciplinary approach (it is not just for Computer Scientists)
Schools	• Teach children to evaluate websites, social media in order to mitigate threats • Include security awareness in the National Curriculum (needs to be driven by the Government)
Businesses and Organisations	• Develop internal role of cyber security; need experienced staff as well as academic knowledge (could be resolved by extended apprenticeships) • Include security awareness and culture in Continuing Professional Development (CPD) for employees
Governments	• Legislation to enable a security culture (as for Health and Safety, or Equality and Diversity)

3.2.2 Findings from interviews

Somewhat orthogonal (at least in terms of the means of data acquisition) to the information on gaps as perceived by the organisations at our workshops, is the information we have gleaned from the structured interviews of teaching staff (in particular, directors of learning and teaching, and lecturers) at the two universities. These interviews were to ascertain what was already being taught and – more importantly – what was not. We asked:

- for background details of the role of the interviewee in teaching
- whether their graduates ought to have an appreciation of the threats and risks of cybercrime and terrorism

- for details of any programmes, modules or lectures that would increase a student's awareness, understanding or skills relating to cybercrime/terrorism
- about any future curriculum developments that would increase coverage of cybercrime/terrorism issues

This effort is currently still ongoing, but a review of the questionnaires and interview reports obtained thus far enables some significant initial findings to be reported here:

1. There was, essentially, universal agreement that it was highly desirable for all graduates emerging from academe to have an appropriate level of understanding about threats to critical infrastructure, organisations, society and themselves.
2. With some notable exceptions, the responses have indicated quite limited (sometimes none) attention to cyber security and counter-terrorism in currently taught material. A standard response from a number of disciplines was along the lines of "The syllabus is already very full; we must focus on material that is explicitly discipline based; these security-related issues are more about life-skills than discipline knowledge".
3. More positively, in very many cases it was thought desirable and valuable to increase the prominence given to guidance and protection against cybercrime and terrorism during induction courses – though there is a risk that material covered at the outset of a 3-year programme may have been forgotten by graduation (the risk might be reduced by incorporating the material in a "handbook" or by online provision, but the real solution to this problem is timely refreshment).
4. We noted that varying levels of attention were paid to the cybercrime/terrorism issue during current induction courses. This suggests that a discussion of basic needs, conducted at University level and involving the central IT team, might be very worthwhile – especially if this led to a standard offering being made available with policy recommendations to back its inclusion.
5. Rather more pointedly, we observed that when a School issues undergraduates with computing equipment for personal use, considerably more attention is paid to ensuring that the student is informed about security threats.
6. There was widespread recognition and agreement that the employability of almost all graduates would not be at all hampered, and in some situations would be greatly enhanced, by the acquisition of security awareness and skills. This suggests that a discussion of skills and capabilities for employment, conducted at University level and involving the central Careers team, would be a worthwhile exercise, and would feed into any outcomes resulting from finding 4 above.

4 CONCLUSION AND FUTURE WORK

Although the work under the SUCCEED project is by no means complete, we feel vindicated that

(i) the employers that we consulted all took the view that they would welcome the opportunity to recruit graduates with a stronger base in awareness, knowledge and skills concerning cyber crime and protection against terrorism, and

(ii) the educators that we interviewed all agreed on the desirability of imparting that stronger base, though curriculum pressure was a strong counter to achieving it.

Thus, our first recommendation will be that universities should give consideration to developing a policy on a basic common level of education and training in this area, developing content with input from security and IT specialists, and having due regard to graduate employability, employers' needs and (not least) the needs of society more generally. Further recommendations will emerge in due course.

This project has been planned as a preliminary investigation; there is clearly scope for validating its eventual conclusions in other HEIs, in other countries, and also for research into how best to address the limitations and gaps we have identified (a range of different approaches can be proposed for this).

And finally, project participants have recognised an "added value" factor in our work, which stems from the different background of the team members at the two Universities. Experience at Newcastle is in engineering and technology for digital security, whereas at Staffordshire the skill set is grounded more broadly in sociological work. These different perspectives have made for instructive and thought provoking interaction.

5 ACKNOWLEDGEMENT

The SUCCEED project is co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union (Project Grant No. Home/2013/CIPS/AG/4000005026).

REFERENCES

[1] Moore, G.E. (2006). Moore's Law at 40, In Brock D.C. (ed.), *Understanding Moore's Law: Four Decades of Innovation*, Chemical Heritage Press PA, pp. 67-84.

[2] Levi, M. & Williams, M. (2012). *eCrime Reduction Partnership Mapping Study: final report*. Cardiff University. http://www.cardiff.ac.uk/socsi/resources/Levi%20Williams%20eCrime%20Reduction%20Partnership%20Mapping%20Study.pdf Accessed 28.9.2015

[3] Scaparra, M.P. & Church, R.L. (2008). A bi-level mixed-integer program for critical infrastructure protection planning, *Computers and Operations Research*, vol. 35, pp. 1905-1923.

[4] Lewis, T.G. (2006). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken, NJ: John Wiley.

[5] Murray, A.T. & Grubesic, T.H. (2012). Critical infrastructure protection: The vulnerability conundrum, *Telematics and Informatics*, vol. 29, pp. 56-65.

[6] Das, S.; Kant, K. & Zhang, N. (2012). *Handbook on Securing Cyber-Physical Critical Infrastructure*. Waltham, MA: Morgan Kaufmann.

[7] Casalicchio, E.; Caselli, M.; Coletta, A. & Fovino, I.N. (2013). DNS as critical infrastructure: The energy system case study, *International Journal of Critical Infrastructures*, vol. 9, pp. 111-129.

[8] Lewis, A.M.; Ward, D.; Cyra, L. & Kourti, N. (2013). European reference network for critical infrastructure protection, *International Journal of Critical Infrastructure Protection*, vol. 6, pp. 51-60.

[9] Biringer, B.E.; Vugrin, E.D. & Warren, D.E. (2013). *Critical Infrastructure System Security and Resiliency*. Boca Raton, FL: CRC Press.