Teaching as a Collaborative Practice: Reframing Security Practitioners as Navigators

Patricia A.H. Williams[1,3], LizzieColes-Kemp[2]

[1] Flinders University, South Australia,
[2] Royal Holloway University of London, UK
[3] Edith Cowan University, WesternAustralia
patricia.williams@flinders.edu.au, Lizzie.Coles-Kemp@rhul.ac.uk

Abstract. The need is growing for a workforce with both technical skills and the ability to navigate existing and emerging information security challenges. Practitioners can no longer depend upon process-driven approaches to people, processes and IT systems to manage information security. They need to be navigators of the entire environment to effectively integrate controls to protect information and technology. The research presented in this paper trialed an innovative tactile learning activity developed through the European Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security (TREsPASS) project with tertiary education students, designed to provide students with experience in real-world modelling of complex information security scenarios. The outcomes demonstrate that constructing such models in an educational setting are a means of encouraging exploration of the multiple dimensions of security. Such teaching may be a means of teaching social, organization and technical navigation skills necessary to integrate security controls in complex settings.

Keywords: Information Security, Security Practitioner, Collaborative Learning

1 Introduction

Information security uses processes, tools and techniques to protect the confidentiality, integrity, and availability of information and information systems. Current information security practice in organizations is carried out through the assessing of risk and performing of risk treatments, the creation of policy and the demonstration of compliance, planning, incident management, and business continuity. Through these actions, the practice of information security management is presented as a systematic approach to the protection of information, and includes people, processes and IT systems.

In government policy [1, 2], information security is promoted as an important means with which to protect an organization's activities and information (assets) upon which an organization relies to undertake day-to-day business. Protection from disrupted business operations, theft of sensitive or valuable information, and reputational damage are important. In the security management discourse there are many examples of the impacts of information breaches [3]. For example, the loss of availability of an IT system for a bank may impact the organisation financially; the exposure of personal health information may breach confidentiality and impact an individual's privacy; and intentional manipulation of student grades challenges the integrity of results.

At the forefront of bringing security know-how into organizations and helping organizations defend against information breaches is the information security professional, often termed "security practitioner". There are many types of security practitioner but broadly speaking a security practitioner helps an organisation to identify and manage its risk from data breaches and attacks on technological systems [4]. Such security professional roles include: IT Security Officer, Information Security System Manager, Information Security System Officer, and Security & Information Risk Advisor [5]. As such, an information security practitioner sits at the intersection between business, technology and regulation. An information security practitioner must also be able to communicate across an organisation with individuals and groups from different educational, professional and social backgrounds.

This paper explores the changing role of information security professionals, security practitioner skills, and conceptualization of security roles, and discusses what is needed in education to respond to these changes. Increasingly, security practitioners are required not only to ensure the protection of technology and information but also to integrate this protection into the wider organizational setting. Such integration requires skills that enable security practitioners to engage with, travel through and bring together the social, economic, political, cultural as well as technical aspects of an organization. This requires building a skill set that sees the security practitioner become both an individual that not only design and deploy information security controls and protection but can also navigate an organization by making sense of the different aspects of an organizational setting, understand the connections between those aspects and communicate the importance of those connections.

In this paper, a re-positioning of the security practitioner as such a navigator of the organization is explored and a navigation visual modelling tool activity trialed. In particular, the work of November et al [6] influences this perspective. In this paper, we reflect on the outputs of a mapping exercise to consider how information security practitioners can construct and use a map of the organizational landscape in order to navigate an organization through risky territory. Whilst the security practitioner is often characterized as a facilitator (e.g. [7]) and technology tools are available that describe the processes of identification and management of risk as navigation (e.g. [8]) the navigation role of the security practitioner is less well considered in the information security practice literature.

The structure of this paper is as follows: in Section 2 information security practice as a profession is discussed, outlining the current skills matrix from the professional bodies, the role of tertiary education and the contribution of November et al [6] to the discussion of navigation as practice and how this conceptualization might prompt a new way of looking at the skills matrix. Section 3 presents the design of a case study that examines how a mapping exercise might contribute to the teaching of the role of navigator. In Section 4 the study results are presented. The discussion in Section 5 includes reflections from the students and facilitators as to the strengths and weaknesses of the navigation approach. This is followed in Section 6 with the conclusion.

2 The Profession of an Information Security Practitioner

Information security has a long and varied history and its evolution shows how information security is an umbrella term for many types of information protection [9]. With the advent of computing, information security became a field of study [10] and as the uptake of computing spread, the field of study has become more diverse. As organizations have become increasingly dependent on computerized production,

circulation, protection and curation of information, information security as a recognized professional practice has also emerged and diversified [11].

2.1 Security Practitioner Skills

Whilst there exist international standards, for instance the ISO/IEC 27000 - *Information Security Management* family of standards [12], and other information security frameworks and guidelines to assess and treat the risks [13], security practitioners must have a range of skills in the processes, tools and techniques of information security. The standards for the management of security [12] emphasize that security practitioners must also have the skills to understand the social, organizational and political context in which these are applied. The traditional methods for managing information security rely on controls of distinct types including those at the administrative or bureaucratic layer of an organization, logical and physical controls within computer systems and architectures, classification of information and information protection techniques such as encryption. These controls are implemented and managed through organizational processes such as governance and assurance, incident response, and business continuity. Within information security practice, there is increased recognition of sociotechnical challenges brought about through ubiquitous computing, big data analytics [14] and the persistent collection of data from the Internet of everything [15]. These sociotechnical challenges can, in one sense, be described as the interactions between the social, organizational and the technical facets.

This awareness of the sociotechnical challenge requires new perspectives on understanding the attack methods, attack phases, continuous monitoring, rapid attack detection as well as the mitigations that are required [14]. The new perspectives that integrate the social and the organizational into what has historically been primarily technical and mathematical thinking require us to rethink our approach to managing information security. In this paper we suggest that one way to reconceptualize security practitioners is to frame practitioners as navigators who chart the organizational landscape anticipating information security harms and plotting a safe and secure course in light of these harms rather than people who simply 'do' information security. As a navigator, security practitioners may oversee the development of policies, the performance of risk assessments and treatments and the design and implementation of security controls. However, their primary role is to help the organization to find a way through the complex and knotty challenges by helping the organization to understand the risk signposts, identify and understand the security relationships between different aspects of the organization, reflect on the potential for information security hazards as the organisation undertakes its activities, and both communicate and collaborate with other members of the organisation to respond to the anticipated risks along the way.

In this reframing, the role of information security education therefore becomes as much about teaching and nurturing navigation skills as it does teaching information security engineering skills. Navigational skills also require an understanding of the broader theoretical concepts of security and the connections between individual, organizational, societal, economic, political and technical securities to understand the complexity of the landscape security practitioners are charting. For example, as the study by Shedden et al [16] illustrates there are significant limitations with current risk assessment methodologies resulting from a lack of recognition of the social and knowledge aspects of organizational processes which are integral to the environment to be protected. It is therefore imperative that we move beyond the teaching of the traditional risk and asset-protection approach to security practice and, instead, teach security concepts, techniques and theories that can be assembled in limitless ways in

real-world environments. Such an education will then enable security practitioners who use their knowledge to read and interpret risk cues and signposts as they navigate an organisation through the complex cyber security environment to meet their business goals and organizational governance requirements.

2.2 Navigating the Risk Landscape

November et al [6] discuss the role of the map in exploring risk landscapes, and eloquently describe using digital technologies both to map terrains and to interact with digital maps in a way that was not possible in the pre-digital age. This interaction enables a community to use the map as a means of navigation and to bring into a single picture both the physical, social, political and human geographical dimensions. The authors argue that such digital mapping techniques liberate the mapping process from being tied to transcribing the physical space as the base of the map and enable the navigator to foreground different perspectives of a space. Digital techniques and technologies, examples of which can be found in [47], enable an individual to map routes through the socio-physical space using a series of risk signposts and building an understanding of the relationship between those signposts. Navigating in this way requires skills to reflect, identify and resolve conflict and to both wrestle with and form a position on ambiguous risk cues that emerge in organizational settings. In this paper, we argue that information security practitioners too have taken on this role of navigator and in so doing must also foreground skills for reflection, conflict management and the resolution of ambiguity. This paper examines one of the techniques that tertiary education in information security might adopt to achieve this.

2.3 Tertiary Education and Cyber Security

In recent years, tertiary education has embraced the teaching of information security. Indeed, governments around the world have encouraged the establishment of new information security courses with a view to increasing national capabilities in information security. The perceived value of information security has been heightened by the shift in framing from information security to cyber security – where the technological aspects of information security are complemented with a political dimension [17]. As part of this shift, a cyber security skills shortage narrative emerges and tertiary education globally has responded to this narrative with a rise in information security courses, often branded as cyber security courses. Cyber security skills shortage has been defined [18] as difficulty to identify and retain appropriately skilled staff for cyber security related roles. Much of the content of such courses therefore focuses on what are regarded as the appropriate skills, namely the technical skills needed to implement secure computers and secure networks. Students enroll on such courses with the promise of future employment. For example, the UK's National Audit Office published a report [19] on the cyber skills shortage in which it estimated that it would take 20 years for the UK to close the cyber security skills gap. This position is reinforced by the ISC2 report [20] that suggests that the difference between the demand driven projection for cyber security workers and the supply constrained projection will be about 1.5 million people globally by 2019. However, the skills gap is largely perceived as an engineering one and whilst there is some focus on governance and assurance skills, these skills are understood through the prism of technology.

In an attempt to refine and differentiate the skills needed for Information and Communications Technology (ICT) and security, the cyber security industry is directing its attention to developing a skills matrix. For instance, the Skills

Framework for the Information Age (SFIA) [21] is an ICT skills and capabilities matrix, designed to align skills with job roles and responsibilities. The framework is careful to distinguish between technical knowledge and professional skills, and maps these skills to seven specific levels of attainment for specific job roles. These levels reflect the amount of autonomy and responsibility expected in each role and consist of: 1-Follow, 2-Assist, 3-Apply, 4-Enable, 5-Ensure and advise, 6-Initiate and influence, and 7-Set strategy, inspire and mobilize. The upper levels, similar to the construction of Blooms Taxonomy for education [22], reflect skills that require industry application such as 'influence'. An essential element of the framework is the experience and qualification, where experience gives practical demonstration of application and consequently capability [21]. Higher education is attempting to embed the practical interpretation of higher-level skills into the curriculum and produce graduates who are job-ready [23, 24]. This is the behest of both the cyber security industry and the students themselves [25] and poses a significant challenge for higher education in how to achieve this [26].

At the same time, the SFIA framework is used by accreditation and professional bodies worldwide to ensure a shared understanding and commonality of language across industry for defining for IT based and associated jobs, the roles and responsibility skills, including those applicable to security. Interestingly, all security related skills are listed at SFIA level 3 and above. Information security skills are levels 3 to 6, information assurance skills at levels 5 to 7, and security administration at levels 3 to 6. This indicates that mere rote learning and understanding of skills is not sufficient. University degrees help students develop generic higher-level skills yet "many struggle in the labour market", "University IT graduates are not well matched with workplace needs", and "In IT, universities are not supplying the graduates needed by a fast-moving industry" [25].

Frameworks such as SFIA have been used internationally to map specific skills to job roles. For example, the Australian Computer Society [27] identified the skills required for twenty-five common ICT roles. This included an ICT Security Specialist for which 61 different skills are needed with skill levels predominantly at SFIA level 5 and above. Other roles across the ICT spectrum were also identified as requiring security skills, such as the role of Network Administrator. When broadening the skill base to include IT governance, of which security is a component, the number of higher level roles with associated high-level skills (SFIA 7) demanding these skills expands rapidly.

Similarly, in the UK, CESG/National Cyber Security Centre (NCSC) [5] has mapped SFIA and the Institute of Information Security Professionals (IISP). For roles, such as Security and Information Risk Advisor, IT Security Officer, and Communications Security Officer, CESG/NCSC defines three levels of role aligned to SFIA level 2, 4 and 6. This acknowledges that in some roles entry level abilities can be catered for in roles that assist in application and monitoring of policy [5]. Such a skills matrix highlights the need for practical application and understanding of the environment holistically, to enable risk management, policy development and conformance, as well as technical skills. Indeed, technical skills themselves are rarely mentioned.

Despite the mapping attempts and skills frameworks, there is still a shortage of appropriately skilled graduates particularly in cyber security. This is due, in part, to the demand for experience (usually five years) in advertised cyber security positions, and a lack of clarity about the skills needed for roles in cyber security [48]. This creates a disconnect between the labour market and the job market, particularly where graduates are concerned. This problem is exacerbated by a lack of recognition of the need for cyber security capability in many organizations, and it is argued that this situation will become critical in the future as organizations realize the need for specialized cyber security capacity [48].

When looking at the governance and information assurance tracks of tertiary education programs in cyber security, it quickly becomes apparent that risk thinking, risk assessment and risk modelling are regarded as significant tracks of the education program [4]. Education in this area focuses on the 'doing' of risk assessment and risk modelling and there is a distinct focus on the protection of information and technological assets and how to achieve this. Within such education programs there is less focus on organizational knowledge, understanding and how information and technological protection interacts with and is shaped by the organizational landscape through which the information flows and in which it is produced. Consequently, our current methods of teaching information security rarely capture this broader perspective, yet it is necessary to be able to understand and apply tools and techniques to the way organizations are experienced and understood [16].

Over the last decade, several voices have articulated the need for change in the education program of information security. For example, there is a view that "academic programs exposing the students to theoretical concepts and problem-solving experience are critical for preparing graduates for jobs in information security" [28]. Equally there is also the view that meeting the requirements for today's information security practitioner, means certifications that focus on vocational training based on core competencies that potentially limit the ability of the student to expand their knowledge base. The difference in tertiary education is that it seeks to elicit broad educational objectives with discipline specific knowledge and academic abstraction [29]. However, whilst voices have acknowledged the need for change in direction in information security education since the turn of the century, the skills gap is still perceived as a largely engineering and technical one and does not include the skills traditionally found in tertiary education that would support the development of a security practitioner as navigator.

A contributing factor to this stalemate in curriculum development is that of the traditional training and certification methods used by the cyber security industry to date. Professional and vendor specific certifications have been popular over the past 10 years. However, in a rapidly expanding and increasingly complex cyber security environment such certifications do not prepare graduates to be sufficiently adaptable. This issue is not new but yet persists. Further, to be at the leading edge of information security protection, education in the field requires innovation and research. Whilst certifications can provide knowledge in the short term, by definition, their content needs renewal periodically and in the cyber security environment this renders knowledge out of date quickly.

2.4 Security Practitioners as Navigators

The University of Queensland and the Australian Information Security Association (AISA) collaborated with the UK's Research Institute in the Science of Cyber Security to conduct parallel studies in the UK and Australia [4, 30] to ascertain the type of work security practitioners undertook and the skills that are needed to undertake that work. From both studies, it was discovered that engagement, and specifically, relationship building and communication, formed the core of a security practitioner's everyday work. It was also discovered that security practitioners wanted new ways of engaging with communities together with clear, evidence-based advice on which engagement methods should be used and when. When the term "community" is used in this context the focus is on groups of people bound together by common characteristics and goals within an organisation. The studies showed that successful engagement is key for a security practitioner because the quality of the working relationship between security and the organization is an important factor in ensuring the effectiveness of cyber security processes.

From both studies it was concluded that information security practitioners often come from an IT background that ill-prepares them for the relationship building, management and communication skills that are needed in real-world security management. In the video summary of the research that forms part of [30], the need to acquire communication skills and capabilities for understanding the cultural implications of technological security is clearly identified. The complexity and highly situated nature of what constitutes information security is highlighted by the diffuse definitions of information security highlighted in the Australian study [4]. The research in [30] articulates the complexity of the organizational setting and the need to navigate and make connections between different aspects of the organization in order to understand the relationships between cyber security technology and the organizational environment. The responses of participants articulated in [4, 30] highlight the centrality of the risk concept in security practice and, yet, how this concept has to hold multiple interpretations of what constitutes the protection of information and technology and how to achieve it.

As both studies show, security practitioners have to develop and maintain specific skills and knowledge beyond the technical, including:

- Skills
    - Communication
    - Conflict identification and management
    - Relationship building and management
- Knowledge
    - Understanding of social, organizational and political as well as technical risk signposts
    - Understanding of the relationship between information security and organizational well-being

This list indicates that to develop good navigators, we need to educate and train security practitioners with good communication skills in order to convince organizations to take and remain on a particular path, strong conflict identification and management skills to keep the organization on course when different communities want to take different risk directions and effective relationship building and management skills keep the organization on the same path, moving in the same direction towards a common risk outcome. These skills, however, are not enough on their own and a wider understanding and appreciation of the world in which an organization operates is necessary. This requires security practitioners to be educated with a theoretical understanding of the security relationships between social, organizational, political and technical aspects of an organization so that security practitioners are not only able to read the risk signposts but to understand the relationships between those signposts. Education of students of information security, therefore, needs to take a broader perspective and a more constructive approach. Whilst it is essential for students to obtain core technical knowledge that enables them to identify, prevent and respond to technical attacks, they must also develop the skills and the confidence to navigate an organization through that complexity when anticipating and responding to attacks on their digital infrastructure.

2.5 TREsPASS and the Navigation Metaphor

To address the difficulty in assessing and identifying the risks associated with the interaction between people and technology, known as socio-technical security, the European Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security (TREsPASS) [31] was established. The project aimed to improve the resilience of businesses and create a standardized framework analyzing the socio-

technical aspects of security. The project [31, 32] developed methods and tools to analyze and visualize information security risks in dynamic organizations, as well as possible countermeasures in response to so-called social engineering attacks where human behaviour as well as technical weaknesses are targeted by attackers. As the project description [31] identifies, examples include StuxNet, in which infected USB sticks were used to sabotage nuclear plants, and the DigiNotar attack, in which fake digital certificates were used to spy on website traffic. New attacks cleverly exploit multiple organizational vulnerabilities, involving physical security and human behaviour.

The navigation metaphor was central to the TREsPASS project [31]. The tools and technologies developed through TREsPASS research [47, 31, 32] were built on the philosophy that security practitioners need to make rapid decisions regarding which attacks to block, as both infrastructure and attacker knowledge change rapidly. Being able to visualize the risk trajectory [47, 32] was regarded as central to these capabilities as the researchers believed that attack opportunities will be identified and prevented only if people can envisage them. In today's dynamic attack landscape, this process is too slow and exceeds the limits of human imaginative capability. The project objectified its navigation metaphor with the development of an Attack Navigator tool to help security practitioners' model which attack opportunities are possible and most pressing, and which countermeasures are most effective.

The project also produced an Attack Navigator Map [47] to help the security practitioner navigate the intended risk trajectory calculation by the Attack Navigator. The Attack Navigator Map presented visualizations that combine information visualizations with techniques from critical cartography and digital humanities to articulate different socio-technical dimensions of risk and provide tools through which to explore these dimensions.

The TREsPASS visualization strategy drew on three types of visualization [32, 46]:

- Artistic visualizations, which foreground the social, cultural, economic and political dimensions to security risks and critique security and risk logics;
- Journalistic visualizations, which situate risks and the data flows within an organization and examine the relationships between those risk pictures and the workings of a risk model; and
- Scientific visualizations, which contribute to the quantification of the qualitative risk data, articulate the attack and defence interaction (for which attack-defence trees are our start point) and enable the user to calculate risk from different perspectives and perform root cause analysis on risks to complex information flows.

Using the TREsPASS tools and techniques, a paper prototype kit was used within two tertiary education programs. The activity provided a hands-on example exploring the physical, digital and social aspects of risk. It promoted the application of risk analysis concepts to a use case. It was not made clear to the students, intentionally, that the basis for the activity was mapping risk analysis approach to the construction of a real-world space. This was only explained to the student after they have undertaken the activity and was part of the post activity whole-class discussion.

2.6 Educational Theory and Methods

Paper prototyping, an output of the TREsPASS [31] research (work package 4 – visualization and tools), was used to inform and enhance education of tertiary students on the construction of security and assessment of risk. This provides an example of

the practical application of security visualization. It further contributes to meeting the outcomes of the undergraduate and postgraduate topics (CSI2102 and CSI5133) Information Security, parts of the Bachelor of Science (Cyber Security), Bachelor of Science (Security), and Master of Cyber Security, at Edith Cowan University, Western Australia. The academic outcomes that this activity in assessing and managing risk contributes to include:

1. Describe and apply concepts, principles and techniques relating to the security of information;
2. Describe the role of risk analysis and contingency planning in information security; and
3. Describe and apply classification systems for information.

Education at the tertiary level in information security has not diverged from the traditional university education model. Whilst there have been attempts at innovative initiatives such as involving students in cyber defense competitions and workflow technology [33, 34] these are not part of the main stream university teaching. There is little doubt that active learning techniques increase student engagement and the use of case studies has been a common method to enact this in information security [35]. However, as articulated in the industry reports, and demonstrated by the increasing emphasis on job readiness using Work Integrated Learning, what is still lacking is the ability of graduates to demonstrate real-world application, in place of experience. The need for students to study and experience complicated information security scenarios, and practice analytical skills is clear.

Paper prototyping has been used successfully as a design methodology for assisting software designers to simulate realistic experience with multiple dimensions [36, 37]. These methods allow identification of real-world issues and provide insights into the environment under study. The application of this method to security education is a novel and innovative approach to learning. It provides a user-centred approach to physical and information architectures and provides the ability to visualize and manoeuvre artefacts representing real situations. Further, if the paper prototyping method include colour coding and physical construction, a multi-method approach, then greater immersion in the task and improved engagement can be achieved [38]. This can provide the learner with experience of situational construction and subsequent analysis, which is vitally important in learning about information security and risk.

It is recognized that the use of visualization methods to assess students in both recognizing security risk and relating this to a specific organizational environment is important in developing an understanding of how being technical and social aspects of risk assessment integrate and impact one another [39]. Based upon General Principle 1. Awareness, skills and empowerments which states that “all stakeholders should understand digital security risk and how to manage it” [39, p.9], it is pivotal or students to gain multiple perspectives on how this can be achieved, starting with how they can construct this for themselves. The development of a solid understanding of digital security risk resulting from the interplay of technology, social factors, physical environment, and organizational process, is vital to the effective management of security in dynamic real-world environments. Further, that effective security requires risk assessment that acknowledges the highly complex and interconnected nature of organisation and information systems [40].

The practice of analytical skills to solve complex problems uses cognitive load theory [41] where the short-term memory is not overloaded in favour of developing longer-term learning skills. Paper prototyping purposefully provides a visual stimulus rather than relying on memory to manipulate an environment and formulate a solution to a complex problem. This approach uses constructivism learning theory with an

instructional design to construct knowledge and meaning from the experience of the prototyping activity. It achieves this using a real-world team simulation thus promoting learning through communication in a safe and supported learning environment. This joint and shared learning experience promotes discussion and negotiation of the task.

Consequently, this approach aligns with cognitive load theory [42] in which the learner is encouraged to optimize intellectual performance. The security concepts used in the prototyping activity are not new to the student in the courses in which the activity was undertaken, and therefore short-term memory overload is minimized. This allows the student to think critically about the task. However, it is acknowledged that there may be some students for whom this method presents limitations where they have not acquired the necessary knowledge prior to the activity. The activity uses a generalized schematic knowledge structure to apply to situational analysis and problem solving, making the skills learned transferable to other problems [43].

3 Method

Three different cohorts of students undertook the paper prototyping activity. In each case the students were given a modelling objective: namely to model the security risks to a sensitive data (in this example exam papers) stored on a server. The students are asked to consider the following when undertaking the activity:

Table 1. Activity guidance

	Consideration/activity construction objective
1	Considering the security disposition of the physical and digital space
2	Identifying the assets and actors
3	Analyzing the security strengths and weaknesses of the assets and actors
4	Producing measures of risk for the threat of unauthorized access mark

This scenario was developed and used because it was a scenario that would be familiar to all students. As a project, TREsPASS worked with several scenarios including the security of ATMs, security of micropayments through IPTV and the installation of malware on memory sticks [32]. Preparation for activity incorporated:

1. Pre-preparing packs of resources for each student group
2. Direction to students regarding readings, lecture, and activity.

3.1 Structure of the Modelling Session

The students were presented with an activity pack containing: a paper prototyping kit and written instructions that replicated the information presented to them by the activity's facilitator. To assess whether the activity can be run independently of the creators of the activity, a different facilitator was used each time the modelling activity was run. Following a lecture on risk assessment, the activity was undertaken in class, with an allocated time of 1.5 hours. The facilitator presented the scenario, presented the content of the packs and presented the activity guidance shown in Table 1.

The students split into groups of between 4-6 participants. Each group was asked to assign the following roles to group members:

- Scribe – notes down the actions of the group.
- Observer – observes the group and checks at the end of the session with the scribe's notes to see if more needs to be added.
- Map constructor – assembles the completed elements as they are made by the group members
- Asset constructor – assembles the asset elements identifying the security strengths and weaknesses of the asset
- Actor constructor – assembles the actor elements identifying the security strengths and weaknesses of the actor (don't forget that attackers are actors)
- Risk constructor – assembles a summary of the risks resulting from the analysis
- All – contribute to the discussion about the values at work.

The following scenario was presented to the groups:

A physical server is used to store sensitive student material, in particular the exam papers for each module. The server is located in the university, in a server room that is protected physically and digitally (via a firewall and host-based security features). The sysadmin employed by the university has full access to the server, two operational administrators have access to the server but not to the exam papers and the module leader has access to the exam papers but not to the underlying operating system. Both the sysadmin and the module leader can edit the exam papers using remote access protocols as well as by locally logging on to the server. The server is logically separated from the rest of the university network (protected by routers and an internal firewall).

The following areas of analysis were outlined:

Please explore the threat of unauthorized access to the exam papers by:

- Considering the security disposition of the physical and digital space;
- Identifying the assets and actors;
- Analyzing the security strengths and weaknesses of the assets and actors; and
- Producing measures of risk for the threat of unauthorized access to the exam papers.

Students were given 1 hour to complete the activities. Whole-class discussion took place for 30 minutes following the completion of the hour. During the hour taken to complete the tasks, groups could ask questions of the facilitator and lecturing staff.

The paper prototyping kit contained lengths of assorted colours that were used to represent physical, digital, organizational and social boundaries. The thickness of the line represented the strength of the boundary from attack. The pack also contained hexagons that were used to represent assets and actors (fig 1). These assets could be decorated in different ways to represent asset qualities (fig 2). In addition, assets were also represented using circles to reflect assets that were protected by other assets (Fig.1).

Fig. 1. An element of the paper prototyping kit.

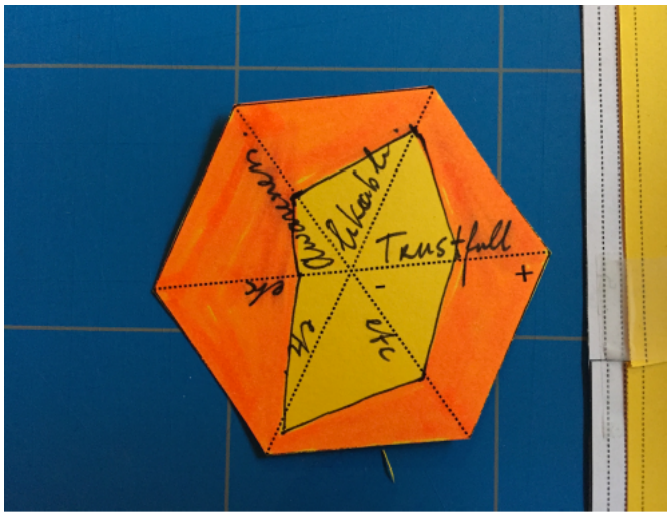

Fig 2. Hexagon to represent assets and their strength

The activity was completed three times over 18 months with information security students on equivalent programs. In each session, data was gathered through photographs taken during the sessions and through annotation of group and whole-class discussions. In addition, reflection feedback was gathered from students at the end of the course and feedback was gathered from lecturers. For this type of activity, there is no model answer as the study is focused on the nature of the process of navigating rather than the results arrived at. Similarly, the analysis focuses on the process rather than the results produced by each student group, although examples of student solutions are provided in Section 4.

4 Results

The student model constructions were analyzed and the results presented in this section. The reflections from students of their learning and from the facilitators is integrated into the discussion section as this relates directly to the synthesis and interpretation of the results. Analysis of the photographs of the group results, together with discussion with the groups during the activity revealed the following general observations:

- Of the four activities the groups were guided to consider (Table 1), analysis of the strength and weakness of assets and actors (item 3) using the specified activity method was overlooked or not considered as important as identification of the factors and how they interacted. The mapping of the strengths and weaknesses using the kite diagram (using up to six parameters) was not undertaken by most of the groups.
- The modelling of the assets and actors was well understood (item 2).
- The concept of using height of the colouring to reflect the magnitude of the vulnerability was not embraced or explored by any group.
- The delineation between the physical and digital space was well understood by the end of the activity, although some students has difficulty conceptualizing and representing the difference between the physical and

digital assets (item 1). For instance, where a server holds the data to be protected.

These observations highlight the limitations of the students in discerning the strength of association between threats. Much of this type of knowledge is learned from experience. As the lecturer feedback demonstrates (given in the discussion), activities such as the mapping exercise are an important means to enable students to consider information security as a multidimensional problem within the class room environment.

4.1 Describing the Physical Space

Students were asked to build a frame to represent the server room in the scenario, to consider the security features of the physical space and to use colour and line thickness to reflect the strength of the space.

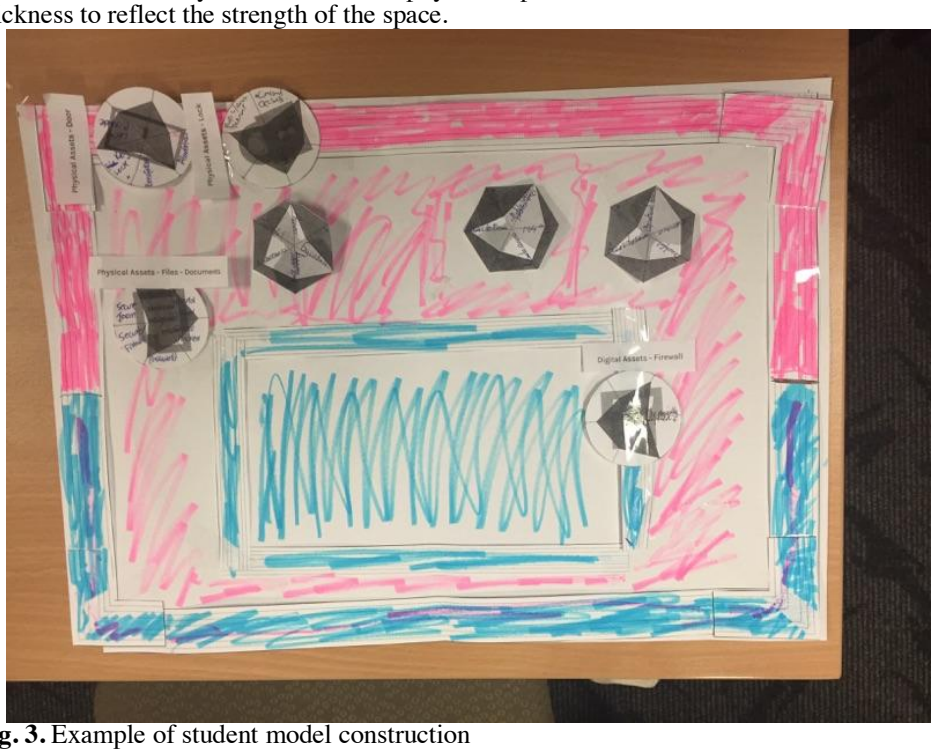

Fig. 3. Example of student model construction

As Figs. 3 and 4 show, the activity was successful in enabling students to consider the interplay between digital (denoted by pink) and physical space (denoted by blue).

4.2 Differentiating Between Physical, Social, Organizational and Digital Characteristics

The activity guidance encouraged students to differentiate between the physical strengths, social strengths, organizational strengths and digital strengths of the server room and indicate these differentiations using colour. By examining the relative strengths of the different dimensions, the students were encouraged to think about

how the different strengths complemented each other and how you might combine these strengths. As Fig. 3 and Fig. 4 show, students were able to differentiate between the physical and digital strengths of a space but found it hard to bring in the third and fourth dimensions, social and organizational strengths, indicating that this is an area that would benefit from future focus during lectures and seminars.

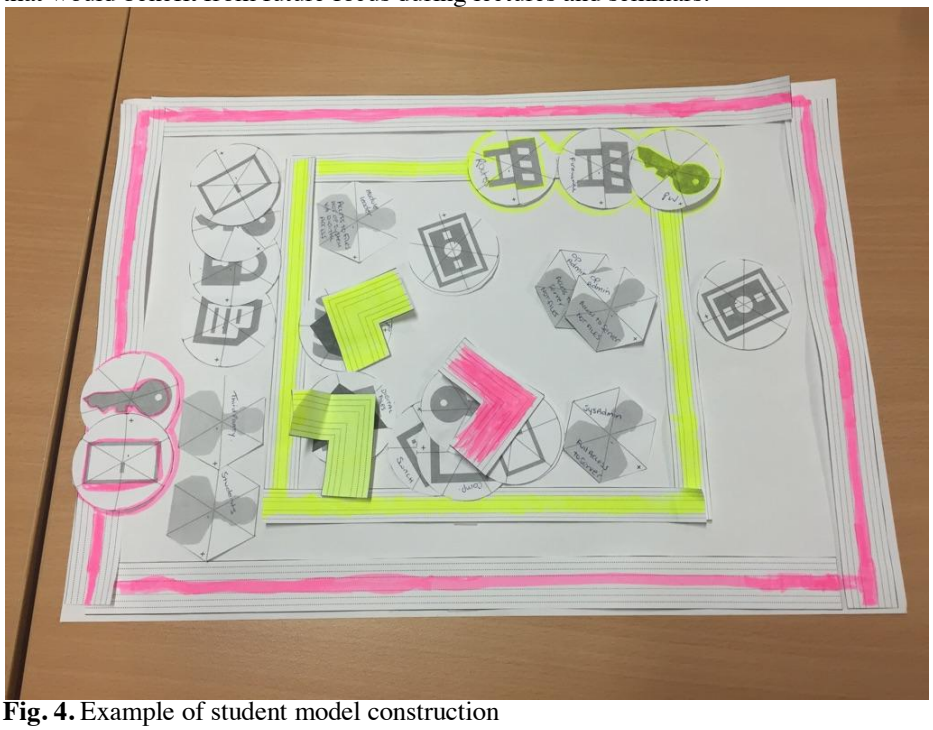

Fig. 4. Example of student model construction

5 Discussion

5.1 Reflection from Students

Students were highly engaged both in the task – particularly in understanding the parameters of the activity and construction of the use case, and in group discussion negotiating what risks were present, the strength of these risks, and how to calculate the magnitude of any risks present (Table 1, item 4). Further, the activity promoted the interpersonal communication required and team work to build consensus within the group. The prototyping activity presents multifaceted learning through personal understanding enhanced by team communication and demonstration through modeling. This method aligns to good cognitive load theory and indeed, Kirschner et al. [44] affirm that groups working on complex problems can spread 'working-memory' across the group thus allowing for enhanced critical constructions.

There were differences, as may be expected, between the function of the postgraduate and undergraduate groups. The postgraduate students took longer to start the construction of the environment using the materials provided – initial discussion

was heavily focused on understanding the use case and getting the solution 'right'. In some ways these students were less adventurous in exploring the activity, with an expectation of providing an ideal answer. This group was more focused on engineering a solution rather than exploring the environment and adapting their responses as they learned more about the environment.

By contrast, many of the undergraduate groups were less concerned with a correct answer, rather focusing on the construction and integration of the elements of the task. In this undergraduate cohort, participants were more willing to combine dimensions of the space they were modelling to develop ways of both understanding and mitigating the risks they were asked to investigate. They reacted to the model in a more intuitive way and examined how the risks were shaped by the environment.

There was therefore a notable difference between the groups who actively started with construction and were comfortable to adapt and change as their understanding of the task changed, and those groups who 'needed' to fully understand all elements before beginning any construction, resulting in them taking longer to understand what they were to achieve and how to go about this. In the former group, there was more evidence of navigation skills, a different type of communication and a more holistic understanding of the system security. It is also noteworthy that the postgraduate groups had a more engineering, solution-oriented approach, an approach potentially learned in undergraduate classes and security practitioner experiences.

The activity provided an alternative method for learning and apply the concepts using visualization. Research demonstrates that "student perceptions of visualization" result in the usefulness of it as a method to address complex issues [45], and in this experience students appreciated the method to enhance their learning. Student comments from the Edith Cowan University – Unit Teaching and Evaluation Instrument indicate that the class activities, including this activity, helped their learning:

- "I found the lecture activities to be the best aspect- I was skeptical at first, but really enjoyed them"
- "Each and every lecture followed by a real-life situation"
- "Being able to utilize real-world scenarios"
- "Out of the box activities"

5.2 Reflection from Facilitators.

"The approach of using a visual representation really "turned the lights on" of the students. The interaction and cooperation of the group was very helpful to the topic, but also for me. I have been trying to get more openness and interaction happening between the students and this was a great way of doing this".

And

"The staged breakdown into "chewable" chunks also allowed for the students to complete a relatively complex task in a logical and methodical manner which takes away the perceived enormity of the task. That said…. For those that went through the process the feedback to me in the tutorial was that when you really drill down its can be quite a complex and thorough exercise, which is what separated a "tick and flick" from "proper" risk assessments."

The students started to think about how the elements connect in the one environment, and this demonstrates a type of wayfinding or navigation. It exposes a method of cognitive reasoning using colouring and different icons that reflects wayfinding and reveals a progression of conceptual understanding about the space on the paper that can be observed as navigating the space under construction.

5.3 Future Activity Refinements

Development of the activity into a 3D space, for instance using Lego, might enhance the activity for those students who need a more tactile experience and who can better identify and make sense of the different aspects of an organization through construction and making. The addition of string to indicate links and weak points might increase the ability of students to define a richer picture and consider an organization in terms of connections and relationships. Whilst consideration of inclusion of the threat sources would be beneficial it is also a limitation given the timeframe allocated to learning sessions. However, including a mechanism for showing physical threats that influence the confidentiality, availability and integrity of information would be a useful addition, particularly for threats from an authenticated insider, as much of the student focus was from the external perspective. Another aspect of complexity that could be added for those with more security experience, or as a follow-on activity, might be highlighting how foregrounding different aspects of an organization (such as social, cultural, economic or political) re-shapes information security risk, and posing the question of how multiple perspectives of risk and information security might be responded to within an information security strategy. This would further highlight the role of the security practitioner as a navigator through increased complexities and nuances of the context under exploration.

In the exercises trialed, students observed other groups working on the problem and the resultant models. In future iterations inclusion of peer presentation of the outcomes discovered would be likely to reinforce learning and to promote discussion and learning by those outside individual groups.

From the outcomes observed, the overlay of the three essential aspects of physical security, logical security and security perception were problematic for some student groups to grasp initially but highlighted to the students the multiple layer and perspectives needed to navigate real-world security landscapes. This aspect of the exercise might be simplified by practice roles to participants, e.g. an information security manager (logical), a CEO (perception) and a physical security manager (physical). The results would illustrate the differences in perspective when all aspects were bought together.

6 Conclusion

The granularity expected to be produced from the construction and analysis appeared to be beyond the cognitive ability of some students with the preliminary level of knowledge and security experience. As part of the cutting-edge EU research on the quantification of risk, and part of the EU TREsPASS project, the students were immersed in concepts designed to prompt thinking as well as make sense of a specific real-world example. The skills and knowledge that such scenarios demand raise the question of whether the traditional risk-based information security practitioner approach to security has reached its ‘use by’ date. There is no argument that the pervasive nature of computing has created complex and technologically interwoven work and home environments, which, in turn, create increasingly challenging problems for effective information security. The role of the security practitioner is evolving, and the expectations of the skills required shifting from purely risk analysis and implementation to that of a person who can see across perspectives and steer a path through the complexities of organizations- in other words a navigator.

Acknowledgments. The researchers would like to thank the participants for their efforts, energy and contributions. Coles-Kemp’s contribution was by supported by the

European Commission through the FP7 project TREsPASS (grant agreement n. 318003). The materials for the workshop were developed as part of Work Package 4 outputs for the TREsPASS project by art studio LUST.

References

1. Australian Government: Protective Security Policy Framework. Australian Government, Attorney-General's Department, (2016), https://www.protectivesecurity.gov.au/informationsecurity/Pages/default.aspx, last accessed 2017/11/30.
2. GOV.UK: Security Policy Framework. Cabinet Office, Government Security Profession and National Security Intelligence. (2014). https://www.gov.uk/government/publications/security-policy-framework, last accessed 2017/11/30.
3. TechWorld: 28 of the most infamous data breaches. (2017). https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/, last accessed 2017/11/30.
4. Burdon, M., Siganto, J. and Coles-Kemp, L. "The regulatory challenges of Australian information security practice." *Computer Law & Security Review* 32.4 (2016): 623-633.
5. NCSC: CESG Certification for IA Professionals and Guidance to Certification for IA Professionals documents. National Technical Authority for Information Assurance, UK. (2015). https://www.ncsc.gov.uk/articles/cesg-certification-ia-professionals-and-guidance-certification-ia-professionals-documents, last accessed 2017/11/30.
6. November, V., Camacho-Hübner, E., and Latour, B.: Entering a risky territory: Space in the age of digital navigation. Environment and planning D: Society and space, 28(4), 581-599 (2010).
7. Coles-Kemp, L. and Overill, R.E. On the role of the facilitator in information security risk assessment. Journal in Computer Virology, 3(2), pp.143-148 (2007).
8. Vasenev, A., Montoya, L., Ceccarelli, A., Le, A. and Ionita, D., Threat navigator: grouping and ranking malicious external threats to current and future urban smart grids. In Smart Grid Inspired Future Technologies (pp. 184-192). Springer, Cham (2017).
9. de Leeuw, K. M. M., Bergstra, J.: The History of Information Security: A Comprehensive Handbook: Elsevier Science. (2007).
10. Saltzer, J., Schroeder, M.: The protection of information in computer systems. Proceedings of the IEEE, 63(9), 1278-1308 (1975).
11. Reece, R., Stahl, B.: The Professionalisation of Information Security: Perspectives of UK Practitioners. Computers and Security, 48, pp.182–195 (2015).
12. ISO.: ISO/IEC 27000:2016 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary. (2016), https://www.iso.org/standard/66435.html, last accessed 2017/11/30.
13. NIST.: Cybersecurity Framework. National Institute of Standards and Technology. (2014), https://www.nist.gov/cyberframework, last accessed 2017/11/30.
14. Giranldi, B., Martin, D., Nguyen-Duy, J., Santana, M., Schwartz, E., Weber, D.: Transforming traditional security strategies into an early warning system for advanced threats: big data propels SIEM into the era of security analytics. RSA Security Brief, 11, (2012). https://www.emc.com/collateral/software/solution-overview/h11031-transforming-traditional-security-strategies-so.pdf , last accessed 2017/11/30.
15. CISCO. Internet of Everything (IoE) value index. (2013), http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe-value-index_Whitepaper.pdf, last accessed 2017/11/30.
16. Shedden, P., Scheepers, R., Smith, W., Ahmad, A.: Incorporating a Knowledge Perspective into Security Risk Assessments. VINE Journal of Knowledge Management, 41(2), (2011).
17. Hansen, L., Nissenbaum, H.: Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53(4), 1155-1175 (2009).
18. Libicki, M., Senty, D., Pollak, J.: Hackers Wanted: An Examination of the Cybersecurity Labor Market. Santa Monica: RAND Corporation. (2014).

19. National Audit Office.: The digital skills gap in government: Survey findings, (2017), https://www.nao.org.uk/report/the-digital-skills-gap-in-government-survey-findings/, last accessed 2017/11/30.
20. Frost and Sullivan.: The 2015 (ISC)2 Global Information Security Workforce Study, (2015), https://www.boozallen.com/content/dam/boozallen/documents/Viewpoints/2015/04/frostsullivan-ISC2-global-information-security-workforce-2015.pdf, last accessed 2017/11/30.
21. SFIA Foundation.: SFIA 5 Framework Reference. (2017), https://www.sfia-online.org/en/sfia-5, last accessed 2017/11/30.
22. Universities Australia.: Landmark strategy to make graduates more 'job ready'. (2015). https://www.universitiesaustralia.edu.au/news/media-releases/Landmark-strategy-to-make-graduates-more--job-ready-#.WEMoFfl97D4, last accessed 2017/11/30.
23. Bloom, B., Englehart, M. Furst, E., Hill, W., Krathwohl, D.: Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain. Longmans Green, New York, Toronto (1956).
24. University Alliance.: Job Ready: universities, employers and students creating success. (2014), http://www.unialliance.ac.uk/wp-content/uploads/2014/07/UA06_JOB_READY_web.pdf, last accessed 2017/11/30.
25. Norton, A., Cakitaki, B.: Mapping Australian higher education 2016, Grattan Institute. (2016). http://grattan.edu.au/wp-content/uploads/2016/08/875-Mapping-Australian-Higher-Education-2016.pdf, last accessed 2017/11/30.
26. Matthews, K.E., Mercer-Mapstone, L.D.: Toward curriculum convergence for graduate learning outcomes: academic intentions and student experiences. Studies in Higher Education, pp.1-16 (2016). doi:10.1080/03075079.2016.1190704
27. ACS.: Common ICT job profiles & indicators of skills mobility: ICT skills white paper. Australian Computer Society. (2013), http://www.acs.org.au/information-resources/ict-skills-white-paper, last accessed 2017/11/30.
28. Hentea, M., Dhillon, H. S.,Dhillon, M.: Towards Changes in Information Security Education. Journal of Information Technology Education, 5, 221-233 (2006).
29. Yasinsac, A.: Information Security Curricula in Computer Science Departments: Theory and Practice The George Washington University Journal of Information Security, 1(2) (2002).
30. Lewis, M., Coles-Kemp, L.: I've Got Something To Say: The Use of Animation to Create a Meta-Story about Professional Identity, (2014), https://www.riscs.org.uk/2014/06/22/ive-got-something-to-say-the-use-of-animation-to-create-a-meta-story-about-professional-identitylewis-m-coles-kemp-l/, last accessed 2017/11/25.
31. TREsPASS.: EU TREsPASS (Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security) project. (2015). http://www.trespass-project.eu/, last accessed 2017/11/20.
32. Coles-Kemp, L.: TREsPASS Exploring Risk. (2016), https://bookleteer.com/collection.html?id=27.
33. Conklin, A.: Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course. In: Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) (2006).
34. He, W., Kshirsagar, A., Nwala, A., Li, Y.: Teaching information security with workflow technology--a case study approach. Journal of Information Systems Education, 25(3), 201+(2014).
35. Zurita, H., Maynard, S., Ahmad, A.: Evaluating the Utility of Research Articles for Teaching Information Security Management. In: Proceeding of Australasian Conference on Information Systems 2015. (2016). https://arxiv.org/abs/1606.01448.
36. Bailey, B. P., Biehl, J. T., Cook, D. J., Metcalf, H. E.: Adapting paper prototyping for designing user interfaces for multiple display environments. Personal and Ubiquitous Computing, 12(3), 269-277 (2008). doi:10.1007/s00779-007-0147-2
37. Tonkin, E.: Multilayered paper prototyping for user concept modeling: Supporting the development of application profiles. In: Proceedings of the International Conference on Dublin Core and Metadata Applications, 2009, pp. 51-60 (2009).
38. Linek, S. B., Tochtermann, K.: Paper prototyping: The surplus merit of a multi-method approach. Forum : Qualitative Social Research, 16(3) (2015).
39. OECD: Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, (2015), http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf, last accessed 2017/11/02. http://dx.doi.org/10.1787/9789264245471-en

40. NIST: Managing Information Security Risk Organization, Mission, and Information System View, NIST Special Publication 800-39, 88 (2011). http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf, last accessed 2017/11/30.
41. Kirschner PA, Ayres P, Chandler P. Contemporary cognitive load theory research: The good, the bad and the ugly. Computers in Human Behavior, 27(1), 99-105 (2011).
42. Sweller J. Cognitive Load During Problem Solving: Effects on Learning. Cognitive Science, 12(2), 257-85 (1988).
43. Kalyuga S, Hanham J. Instructing in generalized knowledge structures to develop flexible problem solving skills. Computers in Human Behavior, 27(1), 63-8 (2011).
44. Kirschner F, Paas F, Kirschner PA. Superiority of collaborative learning with complex tasks: A research note on an alternative affective explanation. Computers in Human Behavior, 27(1), 53-7 (2011).
45. Swords, J., Askins, K., Jeffries, M., Butcher, C.: Geographic visualisation: lessons for learning and teaching. Planet, 27(2), 6-13 (2013). doi:10.11120/plan.2013.00001
46. Hall P, Heath C, Coles-Kemp L, Tanner A. Examining the contribution of critical visualisation to information security. In Proceedings of the 2015 New Security Paradigms Workshop 2015 Sep 8 (pp. 59-72). ACM.
47. TReSPASS mapping tools and techniques for cyber security: https://visualisation.trespass-project.eu/ , last accessed 24/02/2019
48. AISA. The Australian Cyber Security Skills Shortage Study 2016. Australian Information Security Association, (2016), https://www.aisa.org.au/Public/Training_Pages/Research/AISA%20Cyber%20security%20skills%20shortage%20research.aspx, last accessed 2017/11/30.