Preface

Cyber Security, in all its guises, is primarily a male dominated profession with very few women in the arena. The perception that Cyber Security careers are not open to women or are only for those with strong academics in computer sciences has historically not presented the best platform to encourage women to enter the profession or promote the profiles of the few women that are already successful practitioners. The Women’s Security Society (WSS) and the Department for Business, Innovation and Skills (BIS) connected and discussed creating an opportunity to formally discuss the challenges presented to women considering a Cyber Security profession, how to encourage those who may not have considered Cyber Security and the need to establish how women could contribute better to closing the current skills gaps in Cyber Security. To that end a round table was conducted as a first stage approach to better understanding the true source of the problem.

On 1 May 2013, WSS, BIS and the Cabinet Office of Cyber Security and Information Assurance (OCSIA) invited male and female participants from Industry, HMG, Academia and Recruitment to participate in a roundtable discussion examining the challenges and opportunities for Women working within and or wishing to enter a career in Cyber Security. The roundtable was designed to gather insights and experiences from all levels of seniority from entry to CISO in order to consider appropriate strategies that WSS, BIS and OCSIA could develop to address the problems that are the most likely contributory factors to the shortage of women in Cyber Security, and to inform the main themes of a subsequent Ministerial debate.

The WSS would like to thank BIS for their hospitality and support in arranging this event. We also express our appreciation to all the participants in the roundtable for their time, helpful contributions to the discussions, and for their comments in drafting this report. We would also like to thank Natalie Black (Cabinet Office) and Jessica Rushworth (BIS) for their continuing support and for chairing this event.

Jane Wainwright
Executive Board
Women’s Security Society

Clare McBrearty
Board Member for Cyber Security
Women’s Security Society
Executive Summary

The number of women working in Cyber Security roles has not significantly changed in recent years despite a number of initiatives aimed at increasing the number of cyber security professionals to meet the current and future demands of the industry. According to the Office for National Statistics (2013) [A] women currently make up 46% of the UK Labour Market yet the Cyber Security sector continues to remain very male dominated with no significant increase in the number of women choosing Cyber Security as a profession.

An understanding of the full range of factors that underpin women’s decisions not to consider a career in Cyber Security have been relatively unexplored, along with the reasons why the few women who are currently working in Cyber Security roles will continue to progress their career within the profession. This issue is not just for research or academic interest but is essential in ensuring that a greater number of women ascend through a full career in Cyber Security. The WSS organised a roundtable exercise in May 2013 where both males and females from a cross section of Cyber Security roles (Public and Private Sector) and recruitment agencies were invited to participate in a discussion examining the challenges and opportunities for Women working within or wishing to pursue a career in Cyber Security.

This event provided a greater understanding of the issue, and highlighted the likely reasons why women do, or do not consider a career in Cyber Security. Areas such as perceptions of Cyber Security, stereotyping as a career only for IT ‘nerds’, and those assumptions that complex entry qualifications were required to enter the profession were commonplace. Women will generally not apply for roles they do not feel they fit entirely with their experiences or qualifications, and as a result may not attempt to diversify from what they know best. A lack of standardisation and formalisation in career paths and qualifications/training required has also contributed to women choosing not to diversify or enter Cyber Security and given the security arena is historically male dominated across all disciplines, these root causes require engagement to ensure that the industry becomes more diluted as Cyber Security evolves.

Subsequently from the insight gained, a number of actionable outputs have been identified and responsibilities assigned to practitioner, industry and HMG. It is recommended that the findings from the report form the basis for a Ministerial event to encourage onward progression and success from this valuable preliminary exercise.

Women’s Security Society (WSS)

WSS encourages the advancement of women involved in the wider world of security and highlights the needs for a different security professional of tomorrow. The WSS also acts as an inspiring networking forum for women working across the Security Industry
# Contents

Preface.......................................................................................................................................................... 2  
Executive Summary....................................................................................................................................... 3  
Introduction ................................................................................................................................................ 5  
Themes .......................................................................................................................................................... 5  
Participant Selection..................................................................................................................................... 6  
Approach .................................................................................................................................................... 6  
Conclusions ................................................................................................................................................ 7  
Why are so few women working in Cyber Security roles or seeking a career in this profession.............. 7  
What can be done to address these barriers ............................................................................................. 8  
How can these strategies be achieved ......................................................................................................... 9  
  Individuals.................................................................................................................................................. 9  
  Industry Initiatives.................................................................................................................................. 10  
  Government Initiatives.............................................................................................................................. 11  
Recommendations........................................................................................................................................ 11  
References ................................................................................................................................................... 12
Introduction
On Wednesday 1st May 2013, thirty individuals representing a broad cross-section of the Cyber Security world participated in a roundtable exercise held in the BIS conference centre. The main objectives of the exercise were:

1. To gather opinion on the skills and expectations for the female professional working in Cyber Security roles today and in the future.
2. To invite participants who represent a broad section of the Cyber Security sphere to ensure a balanced view.
3. To capture outputs from the exercise that could be used to inform a subsequent roundtable with a view to staging it with participants representing senior professionals within the Cyber space, and/or a Ministerial event.
4. To present four key themes (set out below) to encourage a meaningful discussion around ‘the problem’.

Themes
Whilst the themes discussed could be perceived as gender neutral areas, the focus of the exercise was specifically related to women. The ‘Why, What and How’ were applied against each of the four themes with a view to reducing the cases for each theme into an actionable activity that will enable individuals, industry and HMG to take proactive steps in addressing the issues identified.

1. Skills – What skill sets and personal attributes are required to enter and/or succeed in Cyber Security?
2. Qualifications – What formal qualifications are required in order to enter and/or succeed in Cyber Security?
3. Barriers – What are the issues (perceived or known) preventing entry into or progression within Cyber Security?
4. Opportunities – What are the routes into Cyber Security and how are they promoted?
Participant Selection

In order to ensure that the views presented during the exercise represented as wide a cross-section from across the discipline as possible, the following attributes were identified as the criteria used when participants were selected for invitation.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male or Female</td>
<td>Opinions were sought from both genders as despite the issue being identified as women specific, men are equally as authorised to discuss the subject and therefore in order to prevent bias, participant selection was not based solely on gender</td>
</tr>
<tr>
<td>Recruitment</td>
<td>It was felt that the representatives from the recruitment sector brought knowledge of the current market and the attributes they are asked to consider when selecting candidates</td>
</tr>
<tr>
<td>CISO/CSO</td>
<td>Senior leaders in Cyber Security provided an insight in to what they felt made a successful Cyber Security Professional and were able to advise on the skills and qualifications they look for when building teams or promoting from within their own organisations</td>
</tr>
<tr>
<td>Practitioners</td>
<td>Graduate Entry: Those who entered the Cyber Security profession through academia directly Other: Those who have diversified from other areas of security, IT or sectors outside of Cyber Security</td>
</tr>
</tbody>
</table>

Approach

The participants were split into 3 syndicates, and were purposely selected to ensure diversity in the groups. The themes were presented to the syndicates before they were asked to break-out in to their respective syndicate room and asked to debate the issues presented, with the purpose of capturing the main themes of discussion. Each syndicate had a representative from either the Cabinet Office or BIS along with a member of the WSS board who were the designated facilitators throughout the sessions. A scribe was appointed in each group to capture the thoughts presented during the sessions. The syndicates were required to regroup and present back to one another on the findings captured during their session. Duplicate or similar observations and conclusions were captured as one, in order to ensure the outputs were as succinct and unambiguous as possible.
Conclusions

The following conclusions were drawn from the exercise plenary sessions, and were agreed by all participants.

Why are so few women working in Cyber Security roles or seeking a career in this profession

Despite the increasing number of Cyber Security roles available and rising salaries, many women still do not consider a career in Cyber Security. As it currently exists, the security sector as a whole (considering all aspects of security such as physical and personnel) is a male dominated environment and has been for as long as the sector has been in existence. Therefore, it is not unusual given the current industry demographics that Cyber Security evolved with a heavy leaning towards male practitioners, as many of those without a pre-existing IT background have diversified in to Cyber Security from the more traditional areas of security. Historically the IT sector has also been a male dominated and thus it could be argued that the apparent lack of females in today's Cyber Security industry is a by-product of how both specialist areas are intrinsically linked. It was also felt that like for like recruitment is often viewed as a safe bet when selecting candidates for Cyber Security teams.

Perceptions of Cyber Security range from having a ‘Geeky’ image to a generalisation about what the job entails (i.e. too technology focused and very detailed/technical), leaving many women feeling uninspired and uninterested in entering the profession. Cyber Security is often viewed as being a career path for those who have achieved degrees in a Science or Technology related field and is perceived as only being open to those who appreciate the intricate make-up of an IT Network or could design out Cyber risks through creating and building IT systems. Perceptions of what careers and opportunities are available are often associated with only the technical roles and therefore a career in ‘Cyber’ is generalised for only those who fit the traditional mould and stereotype behaviour set. As discussed by Heilman, Wallen, Fuchs and Tamkins in their research on ‘Reactions to Women Who Succeed at Male Gender-Typed Tasks’ (2004) [B] for women, these typically include behaviours associated with men that are believed to be incompatible with the behaviours deemed desirable for women. Thus, the self-assertive and tough, achievement-oriented, agentic behaviours for which men are so positively valued are typically prohibited for women.

Acknowledgement was given to the impact that the recruitment sector has on perceptions as evidently the vast majority of job descriptions for Cyber Security Roles state that a degree of technical expertise or industry recognised qualifications are required, quite often contradicting what is actually necessary for the role. Therefore, from the outset females tend to disregard such opportunities if they do not possess technical IT skills or have the plethora of certifications required. It was concluded through dialogue with those participants representing Cyber Security recruitment that ‘catch-all’ job descriptions are often advertised in the hope that they will attract a broad spectrum of applicant, however it was discussed that this approach can have quite the opposite effect, as many good female candidates will simply not apply, which is partly due to confidence and an impression that they are not suitable for the role. Discussion led on to suggest that recruiters often find that their clients are unsure as to what their ideal candidate profile is and that there is still
no universal criteria or set of qualifications associated with the plethora of assorted job titles currently related to Cyber Security.

A lack of recognised and defined career paths coupled with an absence of information relating to entry routes in to Cyber Security were mentioned as an additional basis for why there is a lack of women choosing Cyber Security careers.

It was felt that women found it was difficult to truly understand the breadth of opportunities available and how a career in Cyber Security could progress. Opinion was canvassed as to why those who had made a career out of it had found the opportunities to do so and the majority of responses evidenced that Cyber Security has been a career that they had ‘fallen in to’ from a variety of routes and there were very few women who had actually intended on entering the profession from grass roots.

**What can be done to address these barriers**

Changing perceptions was proposed by the participants as an important issue to address. It was felt that projecting a positive and passionate message of women working in Cyber Security roles would help to change the negative perceptions many felt that they had of themselves or how they would be perceived to other women.

Developing coaching and mentoring schemes and opportunities would encourage women working in Cyber Security to develop the skills and attributes required to support them in their roles and to provide them with the confidence to thrive in their professions. The WSS is exploring how they can support this initiative across all security domains and are working with the recruitment sector to better understand how such a scheme may work. Ultimately this would ensure that each individual’s would help to change the perception of themselves and their role to peers and women wishing to embark on a Cyber Security career. Exploiting opportunities to promote women working in Cyber Security will help to progress the championing of women in non-traditional roles and naturally lead to the advocacy of women Cyber Security role models.

It has been well documented [F] that some women are likely to be less confident than men in their careers. Low self-confidence can obstruct women’s career progression and it was clear from the exercise that the female participants were far less likely than their male counterparts to make speculative job applications for Cyber Security roles for which they do not consider themselves fully qualified. Women are more likely to be averse to self-promotion. Low self-confidence also has an impact on the ability to network effectively and often women will require much more encouragement to attend or accept speaking opportunities at events or conferences.

Sharing experiences of women working in different Cyber Security roles would help to address the perception issue, and also build their confidence in public speaking. Women should be encouraged to network within diverse sectors outside the ‘traditional’ Cyber Security sectors (e.g. retail, health, energy, etc) to develop relationships, promote Cyber Security and to connect with women in roles that are non-IT/Cyber Security.
The Cyber Security Challenge (D) is an important initiative for all women working in Cyber Security to get involved in, to promote or support. The aim of the Cyber Security Challenge is to attract more talented people into the Cyber Security Profession, and use a range of competitions to test the knowledge and skills of non-Cyber Security related persons, and promote Cyber Security to those working or studying outside this sector. One such Cyber Security Challenge venture is the schools programme. Women can actively get involved in these competitions either by promoting the competitions and challenges to their local schools, or through their organisations supporting the development of links between the schools, industry and business leaders. This would also provide an opportunity to speak to school-aged girls about Cyber Security opportunities and to challenge the curriculum by providing the links to the practical application used in the Cyber Security Challenge competitions.

Women can campaign for their employers and organisations to address the issue, and to encourage the organisational diversity programmes to specifically develop strategies to promote the opportunities for women working in Cyber Security.

Developing a strategy for a career path, with focus on the transferrable skills into Cyber Security roles is important for encouraging women from unrelated Security roles to consider a career in this industry. Educating and working with recruitment and hiring managers is important to ensure that women seeking to change their career have an opportunity to do so. To encourage clarity of job specifications, change the terminology used and promote those benefits that are important for women working in Cyber Security roles. Taking this approach and preventing the usual ‘catch-all’ job specifications will ensure that more women will take the opportunity to apply and will ultimately help to widen the pool of talent. Preventing HR screening the applicants before their applications reach the hiring manager, or educating them on the selection of good candidates rather than those who must meet the requirements of the ‘must-have’ list.

Other sectors, for example MOD, have conducted media campaigns aimed at increasing the percentage of women working in armed forces roles. WSS could take the lessons learnt from those successful campaigns and tailor the approach to champion women working in Cyber Security. Linking into corporate diversity programmes could also help to promote the issues and encourage industry and recruiting managers to create an environment that embraces women working in Cyber Security, and seeks to create a balance in its workforce.

**How can these strategies be achieved**

Through the workshop sessions a number of initiatives were proposed for Individuals, Corporations and HMG to ensure that the strategies identified to overcome the barriers could be achieved.

**Individuals**

All women should have the ability to be open and honest, to be proud of their achievements and be proactive when seeking opportunities to share their enthusiasm with those they encounter within their professional and personal lives. Women should consider joining organisations, such as the WSS, who actively promote and support women working across the Security Industry to: develop and build trust-based relationships; to
access thought-leadership; and to empower success so that they may progress in their careers and achieve their goals. Acknowledging the contribution that women make to the Cyber Security industry, and celebrating their ideas and accomplishments will ensure that women gain the recognition that they deserve.

Women should look to lend their support to initiatives such as the Cyber Security Challenge through the promotion of the competitions and challenges, to their female peers, family and friends. Becoming a STEM Ambassador for Cyber Security, and provide young girls and women with a role model who is quite different than the usual perceptions of the Cyber Security professional. In this role it is also possible to promote the links between schools and universities to the Cyber Security Challenge to ensure that girls and young women understand that there are opportunities to work in a Cyber Security if they desire.

eSkills [C] provide learning pathways for developing Cyber Security skills, and support the progression of careers from entry level to the highest level of Chief Information Security Officer (CISO). Women working in Cyber Security roles are encouraged to access the report “Career Analysis into Cyber Security: New and Evolving Occupations and to use this as a basis from which to inform the progression of their careers.

**Industry Initiatives**

Corporations have a role to play in having an impact on the number of women filling security roles within their organisations. Industry should develop in-house opportunities to encourage women working in Cyber Security roles and other non-technical disciplines to network.

In line with the Governments strategy to encourage the representation of women at senior levels, industry should provide opportunities for mentoring women at all levels of the organisation, so that it is possible for women to provide representation at a senior board level and become champions and role models to those across the organisation. This strategy would also help organisations to overcome the hurdles and perceptions for recruiting women into roles at all levels of Cyber Security.

Organisations should develop and implement corporate diversity programmes that seek to address the imbalance and demonstrate their support for WSS to promote women in all sectors of security. Development of women-only apprenticeships for Cyber Security roles would help prospective candidates understand that the organisation is a good environment in which to develop their career. Changing the recruitment processes from the traditional routes to so that Cyber Security roles may open up to all candidates rather than a narrow field of specific qualifications or skills.

Collaboration with initiatives such as the Cyber Security Challenge allows organisations to widen their field of perspective candidates, and to develop competitions in order to demonstrate the particular challenges that Cyber Security face.
**Government Initiatives**

Over the years the Government has started a number of initiatives aimed at addressing the imbalance in women considering more technical professions, including IT, science and engineering. With women comprising 45% of the workforce in the UK, the Government needs to support efforts to address this imbalance, and the workshops proposed a number of ways that this could be achieved.

Government departments who operate to support the UK’s development of a Cyber should develop and encourage the formation of STEM Ambassadors with Cyber Security backgrounds.

Pressure should be put on the Education Department, to address the lack of Cyber Security awareness, training and education throughout the National Curriculum, and to develop examinations to test pupil skills and knowledge. This could be achieved by working with Industry and Cyber Security professionals to ensure that the ICT and business related curriculums are developed to include the relevant elements of Cyber Security. Funding should be made available to ensure that the Cyber Security Challenge Schools Competitions may continue and not be wholly reliant on sponsorship from Industry.

For professionals and new entrants, the Government and Industry should promote Cyber Security specific qualifications and pathways into Cyber Security roles. The Government should also ensure that the development of schemes such as the Continuing Professional Development (CPD) promote women’s learning and development throughout their Cyber Security professional careers, and provide a clear career pathway that they can follow to achieve their objectives.

The Government should demonstrate support to external initiatives (e.g. WSS) providing opportunities to collaborate for achieve mutual objectives, and where necessary ensure that there is an opportunity to promote dialogue to discuss those issues where Government and Industry do not necessary agree.

**Recommendations**

Establishing the most likely causational factors for the lack of Women in the profession has provide valuable insights into the professional dynamics at play within the Cyber Security industry. It is recommended that the outputs captured in this report form the basis for a Ministerial event to encourage onward progression and success from this important preliminary exercise.
References


D. Cyber Security Challenge (www.cybersecuritychallenge.org.uk)

E. National STEM Centre (www.nationalstemcentre.org.uk/stem-in-context/what-is-stem)