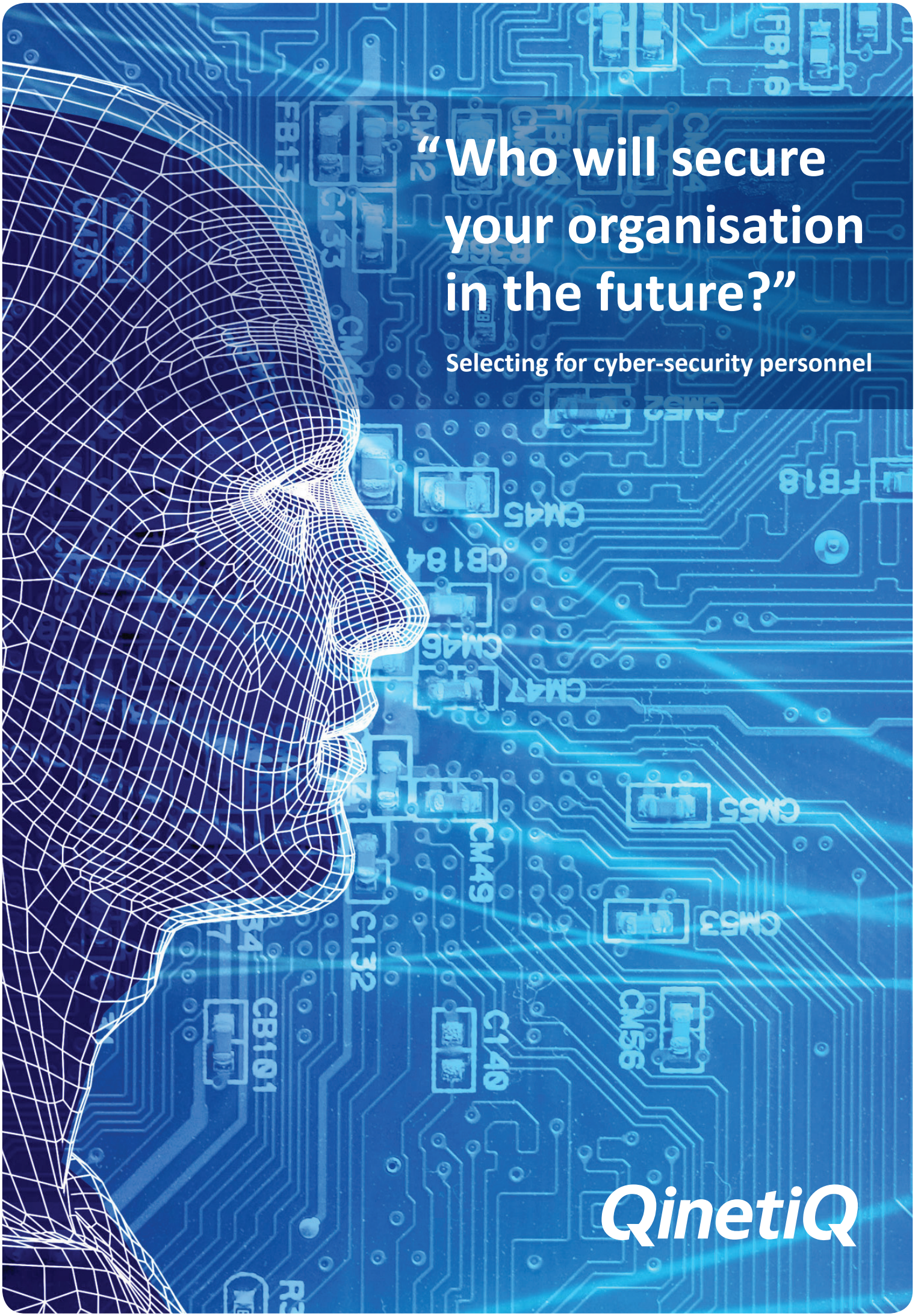


“Who will secure your organisation in the future?”

Selecting for cyber-security personnel

QinetiQ

Cyber-security professionals are predicted to become a 'must have' resource for UK organisations in the next few years[1]. Following the extraordinary increase in Internet usage globally over the past 15 years, from 16 million users in 1995 to more than 1.7 billion in 2010[2], Internet traffic is currently growing at the rate of 60% per year[3]. This will increase our reliance on networked systems, bringing with it an increased vulnerability to the intentional disruption of such systems for political or individual gain. It is anticipated that the UK's cyber-security personnel will be critical because of the role that they will play in protecting money and assets, defending intellectual property, and protecting privacy in online environments.

The need for cyber-security capability within organisations has been highlighted recently with the case of a medium-sized online cosmetics retailer that was hacked consistently over a period of four months before realising that they were under attack. The resultant damage included having to contact their customers to explain that their credit card details had probably been compromised, and an inability to sell their products through their normal distribution channels. The incident is likely to have far reaching consequences to the organisation as they try to rebuild trust and repair their reputation with their customers and corporate stakeholders.

The impact of this breach of security could have been reduced if certain simple measures had been employed. For example, protective monitoring could have detected the breach earlier. Alternatively, the implementation of regular 'Red Team' methodology penetration testing could have identified the weakness in the system prior to the attack, and prevention measures could have been taken. The effectiveness of such measures relies heavily on the skills of the analysis team involved.

Given that approximately 90% of all our high street transactions as consumers are made using credit and debit cards that rely on wired and wireless communication, this is an important issue[4]. It is vital that organisations can give reassurance to their customers that their details will be secure, and knowing that they have the right people looking after their corporate networks is essential for securing these data. According to the 2008 Information Security Breaches Survey conducted on behalf of the Department for Business Innovation and Skills (BIS)[5], in 2008 72% of large businesses reported having had an information security incident, and 68% of large businesses reported a malicious security incident. Nearly 3 in 10 (31%) of large businesses experienced a significant attempt to break into their company network, and just over 1 in 8 (13%) had actually had their network penetrated.

It is predicted that in the future there will be a shortage of cyber-security skills, increasing the probability of more successful attacks like the one described above. It has been suggested that in the US there is a need for 10,000 to 30,000 security professionals to tackle the threats within cyberspace, and that currently there are only about 1,000 specialists with these sorts of skills[6]. Shortages of suitably qualified personnel are also expected in the UK. As Judy Baker, director of the UK Cyber-security Challenge, says:

"We have to improve the quality and quantity of talented people entering the profession to accommodate escalating requirements.

The current system is not delivering enough skilled professionals to meet the cyber-security challenges we face. We need to excite, inspire and stimulate fresh interest in a career as a cyber-security specialist." [7]

Having the right cyber-security talent in place is going to be critical for organisations in the future. At QinetiQ we take recruitment of our own Information Security professionals very seriously. Our employees are working with some of the most complex systems and organisations in the world, where security vulnerabilities can lead to a loss of life, valuable assets, or critical intellectual property. It is essential that they have the necessary skills, behaviours and attitudes to maintain a robust defence against current and emerging threats from cyberspace. We're already planning for this talent shortfall and we'd like to show you how we can spot the talent of the future.

[1] Downing, E. (January 19, 2011). *Cyber-security – A new national programme.* House of Commons Library. Retrieved 9th February 2011, from http://www.parliament.uk/briefingpapers/commons/lib/research/briefings/snsc-05832.pdf

[2] HM Government (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. Norwich, UK: The Stationary Office (TSO). Retrieved 9th February 2011, from http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf

[3] GCHQ *Press Release*, Director GCHQ, Iain Lobban, makes Cyber speech at the IISS, 12 October 2010

[4] Office of Cyber-security and UK Cyber-security Operations Centre. (2009, June). *Cyber-security Strategy of the United Kingdom: Safety, Security and Resilience in Cyberspace. (Cm 7642).* Norwich: The Stationary Office. Retrieved 9th February 2011, from http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

[5] Department for Business Innovation and Regulatory Reform (2008). 2008 Information security breaches survey. Retrieved February 9, 2011 from http://www.bis.gov.uk/files/file45714.pdf

[6] Gosler, J. (July 19, 2010). Cyberwarrior shortage threatens U.S security, *NPR Morning Edition, July 19, 2010.* Retrieved 9th February 2011, from http://www.npr.org/templates/story/story.php?storyId=128574055.

[7] Beaumont, C. (2010, April 27). Government backs competition to recruit security experts. The Telegraph. Retrieved January 17, 2011 from http://www.telegraph.co.uk/technology/7638185/Government-backs-competition-to-recruit-security-experts.html

What if you had to invest in one of these individuals for the future of your organisation, who would you choose?

Meet Kevin.

Kevin is just completing his A-Levels and desperately wants a career in IT security, having been offered a place to study Computer Science at university. Kevin spends much of his spare time at home developing his IT skills, is a member of a number of computer-related societies, and last year attended the Information Security Europe conference.

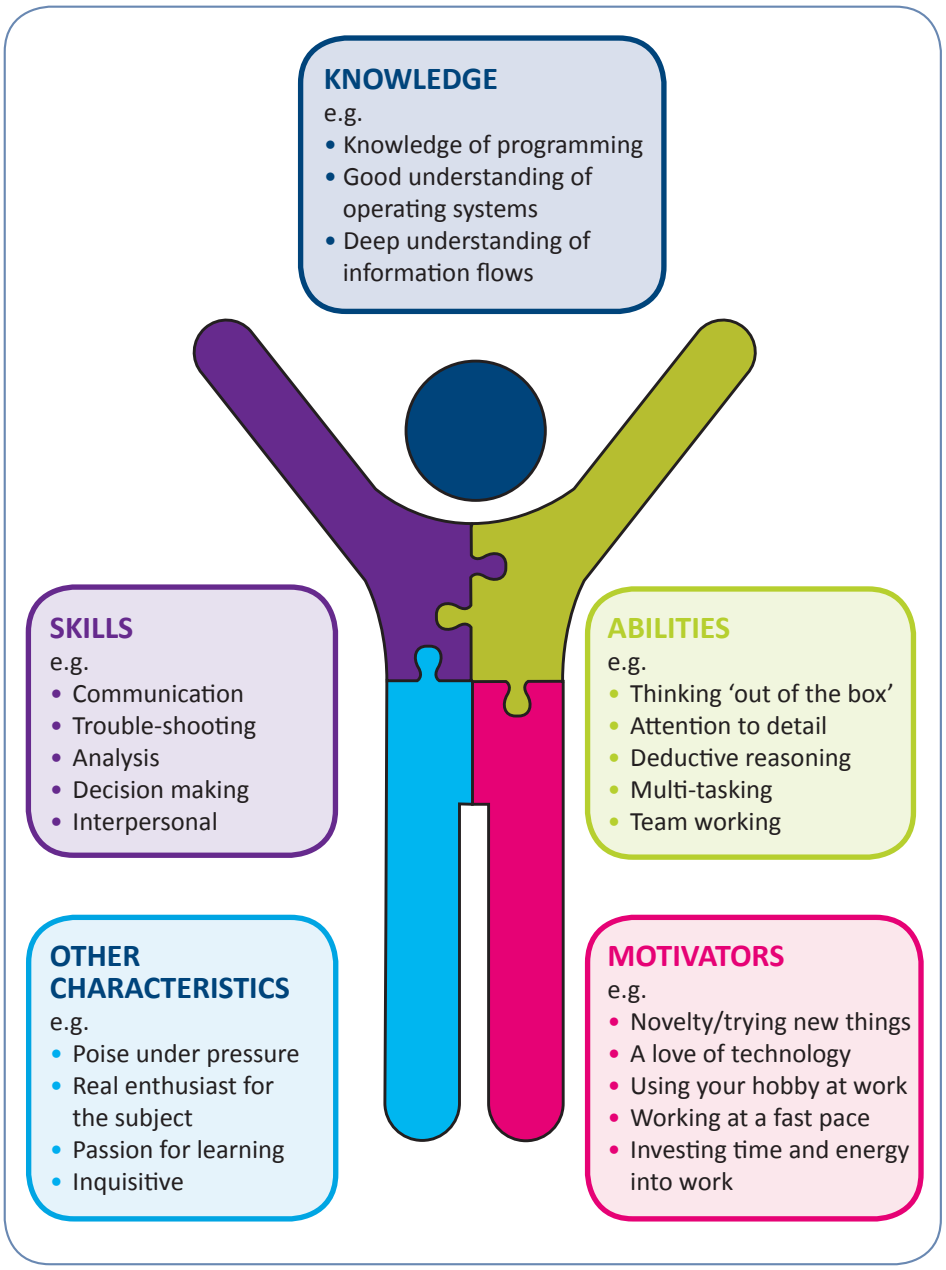
Meet Clare.

Clare is also completing her A-Levels. Last summer she attended a computer science summer school run by Cambridge University, and is now developing her computer skills in her own time with students she met at the summer school. In addition, she also plays netball, is on the student committee at college and organises events for a local charity.

The importance of understanding the requirements of the job

If we were choosing between Clare and Kevin as one of our future cyber-security professionals then the first thing we would do is look at the demands of the job we wanted them to perform. From this we would then look to analyse what sort of person we needed for the role, and to do this we would identify and select the competencies that Clare or Kevin will need to demonstrate to be successful in the role.

Our experience of doing this type of activity is extensive and we've done it many times for roles as diverse as bomb disposal personnel to airport security officers. In fact, we've recently done this exercise to define the personnel requirements for the future cyber roles within a Government department and also for the assessment of finalists in the UK Cyber-Security Challenge. What we found was key cyber-security skills in the future will include a combination of knowledge, skills, abilities, other characteristics and motivators (a sample of which are shown in the diagram below). Being an effective cyber-security professional involves more than just applying technical skills: it also involves working well in a team, making effective decisions, using information appropriately, and responding quickly to issues that arise. The importance of these additional non-technical skills was recognised in the 2009 Cyber-security Strategy for the United Kingdom[8].



[8] Office of Cyber-security and UK Cyber-security Operations Centre. (2009, June). *Cyber-security Strategy of the United Kingdom: Safety, Security and Resilience in Cyberspace. (Cm 7642).* Norwich: The Stationary Office. Retrieved 9th February 2011, from http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

Assessing talent

Okay, so we know what we need from an ideal candidate, how do we choose between candidates such as Clare and Kevin?

In an ideal world we'd give Clare or Kevin the opportunity to demonstrate that they can cope with the demands of the job by either getting them to sit psychometric tests, or ideally by giving them a sample of the type of work they would face on the job. At the recent Network Defence Competition of the UK Cyber-security Challenge we did just that. The four finalist teams, shortlisted from over 500 entrants to the competition, were given an opportunity to demonstrate their skills in defending a simulated network, typical of an average UK home or small business. The facility QinetiQ created allowed the teams to compete against each other in a series of technical challenges. Each was designed to allow the participants the opportunity to demonstrate the competencies that we determined were important. With a team of our Information Security experts and Occupational Psychologists we were able to objectively assess them in action against each of the target competencies. Whilst our Information Security experts were able to assess their technical skills, our psychologists, who are experts at observing, recording and classifying instances of behaviour, were able to assess the non-technical behaviours that the competitors demonstrated throughout the day.

Choosing the best Information Security specialist

From our experience of selecting cyber-security professionals, we know that whilst specific technical knowledge and skills such as awareness of operating systems, firewalls and routers are important, many of the characteristics that are required for these roles are what might be termed 'softer' behavioural skills (e.g. ability to work well in a team). In the UK Cyber-security Challenge we found that the teams were fairly evenly matched in their ability to cope with the demands of the challenges from a technical (cyber-security) point of view. However, there was a big variation in performance on the behavioural skills. The table above shows an example of some of the behaviours observed.

When a team worked together well and remained focused at times of increased pressure during the competition, they were also able to make best use of their technical skills. The successful teams were organised, with leaders who were able to assign tasks according to team member strengths, could share the monitoring of the network for attacks so that no one person became overloaded, and were able to support each other in order to develop and execute the most appropriate responses. It was a combination of their technical abilities and their behaviours that enabled them to apply their knowledge and technical skills more effectively. Even in a situation where a candidate's technical skills are marginally better than another's, if they do not also demonstrate target behaviours, we are unlikely to select them as a cyber-security professional.

	Most successful teams	Least successful teams
Make decisions and initiate action	• Formulated a clear plan and stuck to it. • Made prompt decisions when needed.	• Started with a clear plan, but then did not follow it. • Hesitated when making decisions and over-analysed the options.
Work effectively with others	• Encouraged each other verbally. • Checked each others' progress on tasks and offered helped when required. • Had an awareness of each others' emotional reactions. • Assigned tasks according to team member strengths. • Brainstormed ideas as a group.	• Did not notice when other team members were stressed or under pressure. • Often worked independently. • Often had heated debates/ arguments with each other (e.g. when discussing technical solutions to particular problems).
Analyse information effectively	• Made good use of all available information. • Shared information across the team. • Gave due consideration to the customer's requirements.	• Focused too much on technical detail and lost the bigger picture. • Failed to consider the end result that was needed.
Adapt to change	• Approached change as an interesting new challenge to be tackled.	• Responded to change as a hindrance to achieving existing tasks
Cope with pressure	• Responded positively as workload increased when the network came under attack.	• A state of panic was evident when the pressure mounted (e.g. time pressure; multiple tasks). • Expressed frustration that things were not going to plan. • Focused too much on what was going wrong, and not enough on the other ongoing tasks.

We believe that having the whole package is more important.

Choosing the wrong person

At QinetiQ we understand if we make the wrong decision when choosing between candidates then this can have a significant financial impact. The Chartered Institute of Personnel and Development estimate that the recruitment costs alone for an average UK worker are now £6,125 per hire. If we were to recruit Kevin and then decide that we didn't want him then that would instantly cost us £12,250: the cost of recruiting Kevin, plus the cost of recruiting his replacement. We could also add costs associated with any training we've given to Kevin and any

remuneration by the time we make our deselect decision plus any compensation arrangements associated with him leaving the organisation. As well as the personnel-related costs, there are also other financial implications associated with having the wrong person within a cyber-security role, which can be incurred if security breaches occur. According to the Department for Business Innovation and Skills (BIS)[9], the average total cost for an organisation's worst security breach is £10,000 - £20,000, rising to an average of £90,000 - £170,000 for large organisations, and up to £1-2million for very large organisations. So it is clear that making errors, and/or failing to identify and mitigate threats, can have serious financial implications, not to mention the potential reputational damage that can follow. For certain organisations the risk is even greater: recruiting the wrong person into roles where security vulnerabilities can lead to a loss of life or valuable assets for our clients, is a risk we are not willing to take.

So who did you choose: Clare or Kevin?

Whilst Kevin clearly has a strong interest in computers, and his background suggests he may have a number of the skills that might be expected for a future cyber-security professional, Clare's extra-curricular activities and experiences should not be underestimated. Being an effective cyber-security professional involves more than being technically competent: it is about being an effective team member, even when working under pressure.

You've selected the right person, what next?

Selecting the right people for cyber-security roles is the first step in enhancing an organisation's security performance through its people; however, to maintain performance, it is important to continually assess the extent to which all personnel are behaving and performing as expected in relation to cyber-security. Whilst it is true that many of the cyber threats facing organisations come from outside of the organisation (e.g. viruses, advanced persistent threats (APTs), dedicated denial of services (DDoS) attacks, hackers), the threat posed by personnel working inside the organisation should also not be underestimated. We recognise that an organisation's personnel represent both the best line of defence but also the greatest security vulnerability. Insider threats may either be unintentional or deliberate, and may come directly from cyber-security personnel or from other employees who use IT equipment: identifying those who pose a risk and acting early, prevents employees from taking misguided actions and protects organisations from attack. Therefore, understanding the insider threat and how to mitigate it (e.g. through appropriate staff care) is a key consideration for organisations. This will be the focus of our next white paper.

QinetiQ's Operational Readiness team

QinetiQ's Operational Readiness team works with security and safety critical organisations, where mistakes can lead to loss of life, valuable assets, or intellectual property, or to serious reputational damage. We optimise how our clients' people, processes and equipment interact to enhance performance, save money and reduce human error. This is achieved by working closely with our clients to understand their needs, their system and their goals so that they can achieve their objectives. Our experts in selection and assessment work to help our clients understand how to optimise their performance by recruiting and retaining the best talent.

Paula Glover BSc MSc CPsychol

Senior Consultant, QinetiQ

Paula is a Chartered Occupational Psychologist and is also an Associate Member of the Chartered Institute of Personnel and Development (CIPD). Paula has ten years of experience working in the fields of Human Resources (HR) and Occupational Psychology, working for six of those years at QinetiQ. Paula has a strong track record in selection and assessment delivery and research, working with organisations to recruit and retain top talent. For example, she currently delivers assessor training to Board Members at Royal Navy's Admiralty Interview Board and also delivers Level A (ability testing) training to Army recruiters, to help maximise the effectiveness of selection into safety and security critical roles in the Armed Forces. Paula also conducts personality-based assessments for the selection of bomb disposal technicians for the British Army. In 2010, Paula developed the behavioural assessment criteria for the Network Defence Competition stage of the UK Cyber-security Challenge, and she was one of the assessors during that competition. Paula is also currently working with a Government department, identifying future skills requirements for cyber-security professionals, a topic on which she recently presented at the 2011 Information Security (InfoSec) conference in London.

Simon Bowyer BSc MSc CPsychol

Senior Consultant, QinetiQ

Simon Bowyer is a Chartered Occupational Psychologist with ten years' experience in helping organisations select their talent efficiently, effectively and fairly. Simon's previous work includes teaching best practice in selection and assessment at both the Army School of Recruiting and Royal Navy School of Recruiting, as well as for the Royal Navy's Admiralty Interview Board. Simon has also developed a revision of the National X-Ray Competency test for Airport Security screeners and led a best practice review of the National Firefighter Selection process. Additionally, Simon conducts personality-based assessments for the selection of bomb disposal technicians for the British Army. Simon was also an assessor in the 2010 Network Defence Cyber-security Challenge where he identified the cyber talent of the future.

[9] Department for Business Innovation and Regulatory Reform (2008). 2008 Information security breaches survey. Retrieved February 9, 2011 from http://www.bis.gov.uk/files/file45714.pdf

QinetiQ