Wanted: the new cyber-warriors

A growing cyber-threat means that the need to hire the best recruits to protect against it, both from traditional and new backgrounds, has never been greater. **Chris Price** reports

The pace of technological innovation in business has brought massive benefits, enabling us to bank at the touch of a button, share information faster than ever and giving us the freedom to work more flexibly.

Yet while making our lives easier, technology has brought a number of challenges being tackled by a growing cyber-security industry. According to UK government figures, the cyber-security sector is worth more than £6bn and employs 40,000 people. In addition to national demands, the cyber export market grew from £850m to more than £1bn during 2013 and is expected to reach £2bn by 2016.

As the industry grows, the need for businesses to recruit and retain people with the right skills to deal with the cyber-threat has never been greater. That was the key finding of a panel of experts brought together recently by BAE Systems and *The Daily Telegraph*.

"Our customers are facing a very sophisticated level of threat," said Nigel Whitehead, group managing director, programmes and support, of BAE Systems, which provides cyber-security solutions to private companies and national governments. "Those posing this threat are either operating at a national level, are involved in organised crime or casual crime, are seeking publicity, or simply doing it for the thrill." Whatever the motivation behind these crimes, the cyber-security industry recognises the importance of recruiting talent to protect businesses and individuals against this threat. BAE Systems recruits about 800 apprentices and 300 graduates a year, with around a third of the graduates going into its cyber-security Applied Intelligence business.

TALENT

The expert panel believed it was not only IT-savvy specialists who were required to deal with this security threat. Employers are looking for people who can learn quickly, adapt to changing situations, and who are naturally curious. Mr Whitehead added: "The ability to communicate often very complex issues to people who might not be so well versed is essential."

As well as finding the right people through training schemes, successful cyber-security teams often have talent from a number of professions – bright individuals with a natural aptitude to learn. Although the workforce currently has a significant proportion of IT-savvy males, the panel believed there are areas of cyber-security that can help broaden its interest to other groups, such as through its relevance to law, international politics and psychology.

One organisation playing an active part in helping people to bridge employers' skills gaps is the UK Cyber Security Challenge. It organises competitions and challenges that attract thousands of contestants from which companies can then recruit cyber-security professionals.

Growing threat
Dealing with cyber-security has led to the cyber export market growing from £850m to more than £1bn two years ago and is expected to reach £2bn by 2016

In one challenge this year, 42 "cyber-defenders", whittled down from thousands of hopefuls, tried to stop "cyber-terrorists" taking over the navy cruiser HMS Belfast in a simulated attack.

Dr Robert Nowill, who chairs the UK Cyber Security Challenge board, said: "We are looking to find people who can join the industry. That might be people in schools and universities thinking about it, or people who have never really considered it. It may even be people who are engaged in unethical hacking who would rather do ethical hacking."

GCHQ, the UK government intelligence agency, runs two summer camps. One is held in Cheltenham for about 80 students who have mainly studied STEM subjects; the other, which takes place in Scarborough, for around 40, attracts a more diverse group of backgrounds. It is also looking at how to use masters degrees to bring people into the cyber-security industry from new routes, perhaps in mid-career.

IMAGINATION

Undoubtedly one problem with recruiting relevant staff is in defining cyber-security. Although often used as a catch-all term, it actually comprises several elements. "Traditionally everybody was very broad in their skill sets. They were either technical or non-technical," Christian Arndt, director at PwC, cyber-security leader and technologist, told the panel. "As the topic has got more complicated it's not one or the other, there are probably seven or eight distinct career paths."

Cyber-security skills include being able to implement and manage robust security systems as well as planning and designing components so organisations can reduce the time spent fixing bugs and holes. However, creative skills are also often required as security professionals adapt legacy systems and help organisations respond to change.

For Peter Allwood, a senior business leader at MasterCard's Enterprise Security Solutions business, cyber-security careers demand creative minds. "It's about having the imagination to understand how attacks work and to develop new security solutions that can strike a balance between being secure and usable."

MasterCard is currently looking at biometrics for banking authentication, and aims to recruit people who are passionate and curious about cyber-security who can pass on their knowledge to others within the organisation.

A key concern of panellists was representation at board level, often in the form of a chief security officer. Although IT professionals are often thought of as operational people, soft skills are needed to explain the risk to others, particularly at senior level. Terry Greer-King, director of security for Cisco UK and Ireland, said: "We need to find the ability to communicate what cyber-security means in a business risk context at board level. You are almost looking for a philosopher-warrior type who can bridge the technical and business worlds."

Dr Yiannis Pavlosoglou, strategic change manager for operational resilience at financial services firm UBS, said: "We're looking for people who can be part of a broad conversation, but be able to contribute to an operational meeting."

For Natalie Black, director of cyber-security and information assurance at the Cabinet Office, it will become increasingly important for everyone to have at least basic cyber-skills: "The reality is that all professionals, all managers, will need to be a cyber-security professional in some form… to be able to talk to their security experts and challenge from a board perspective."

With a budget of £860m over five years, the Government's cyber-security programme aims to ensure all school leavers have a basic understanding of what cyber-security is. Richard Kenworthy, an apprentice at BAE Systems Applied Intelligence division and a recent graduate, noted that IT courses in schools do not currently cover cyber-security. "I did an IT course in the sixth form in which there was a little bit of development and a lot of project management and evaluation. But nowhere was cyber-security even mentioned."

While many companies are employing relevant graduates and apprentices, there is still a need to plug the growing skills gap in the industry at a much younger age.

For the past 10 years, BAE Systems has been doing a schools roadshow. This year, 300 schools took part in a display in which subjects such as maths and physics are brought to life in the assembly hall. "It starts in Years 6 and 7," Mr Whitehead said. "If you can inspire someone to be interested in maths, technology, science and computing before the topics become complex, it gives them a reason to study those difficult subjects."

According to Dr Guy Bunker, senior vice-president at Clearswift, cyber-security has grown into an issue beyond businesses, relevant at home. "It should be taught in schools about why you need to protect your information," he said.

MOTIVATION

The shortage of relevant skills now and in the future goes beyond a recruitment problem. With talented individuals in short supply, holding on to them can be challenging for employers. This is especially true with "penetration testing" (often known as ethical hacking), where two years would be considered long-term employment. Foreign companies are offering much higher salaries to tempt workers overseas.

To help with the retention of these creative and increasingly expensive individuals, Clearswift assigns Tuesdays to people to allow them to work on their own creative ideas within the company. Some of these may be related to what the individuals are doing day to day but it could equally be a project that is more "blue-sky thinking".

BAE Systems has a virtual Applied Intelligence Lab where anyone in the organisation can suggest an idea that could become a product. "It helps people at all levels stay connected with the business," Elaine Baker, who is engineering director at BAE Systems Applied Intelligence, told the panel.

Yet another key consideration for retention is to demonstrate long-term career prospects within an organisation, or the industry as a whole. The Institute of Information of Security Professionals helps to provide a clear framework for those working within cyber-security, so they have an idea of what they should be achieving at each level as their career progresses. "We need to articulate what the career path is, to give people a reason to stay in particular role," Mr Whitehead told the audience.

For Mr Allwood, successful staff retention is also about having a dialogue with personnel. "You need to have engagement about what they do in their role and you need to rotate roles to a degree. "Spending time in different roles and allowing people to find out where they work best will hopefully mean they stay longer. It's good for the individual and good for us, too."

CYBER-SECURITY ROUND TABLE

Chris Hankin
Director of security of the Institute for Security Science and Technology, Imperial College London. Chair of the round table

Nigel Whitehead
Group managing director, programmes and support, BAE Systems

Elaine Baker
Engineering director, BAE Systems Applied Intelligence

Dr Robert Nowill
Board chairman, UK Cyber Security Challenge

Terry Greer-King
Director of security, Cisco UK and Ireland

Christian Arndt
Director at PwC, cyber-security leader and technologist

Natalie Black
Director of cyber-security and information assurance, Cabinet Office

Chris Ensor
Technical director, CESG (GCHQ) and head of profession for information assurance

Peter Allwood
Vice-president, senior business leader, enterprise security solutions, strategy, MasterCard

Guy Bunker
Senior vice-president, Clearswift

Yiannis Pavlosoglou
Strategic change manager for operational resilience, UBS

Richard Kenworthy
Apprentice, BAE Systems Applied Intelligence

Read the full discussion and view video clips hosted by BAE Systems at **telegraph.co.uk/inspiringSTEM**

BAE SYSTEMS
INSPIRED WORK