Plugging the cyber-security skills gap

Tracey Caldwell, freelance journalist

It could take up to 20 years to address the cyber-security skills gap, according to a National Audit Office (NAO) report published in February 2013.¹ This has translated into a dangerous dearth of skills in organisations.

An E-skills survey of CISOs with 40 employers found that 85% of organisations experience recruitment problems as a result of not enough candidates with the right cyber-security skills. According to the NAO, the government is working to address this and has said that it intends to overhaul ICT teaching in schools to make it genuinely about computer science rather than office skills. It expects cyber-security to be a strong strand of the future GCSE computer science syllabus. But for now, this shortage of ICT skills hampers the UK’s ability to protect itself in cyberspace and promote the use of the Internet both now and in the future, in the view of the NAO.

“If organisations don’t have employees with the skills needed to fight back at cyber-criminals, we will be fighting a losing battle. This will ultimately lead to fewer jobs all round as businesses suffer the repercussions of cybercrime.”

He adds: “With cybercrime costing small firms £800m a year according to a report conducted by the Federation of Small Businesses, now, more than ever, we need a fully equipped cyber-security workforce. Online attacks on small businesses bleed money from our economy straight into the hands of criminals.”

Howard Skidmore, technical lead for information security and cyber, e-skills UK, says: “When organisations do not have the skilled professionals needed to secure their systems, they face a variety of risks, including the loss of intellectual property, financial information or personal data, which can attract heavy ICO fines and cause significant reputational damage. As such, it is good business sense to invest in cyber-security skills before an incident – the cost will be the same after a breach, but the damage will have been done.”

There is evidence that employers are waking up to perhaps the biggest risk to the security of their operations. The PWC 2013 Information security breaches survey was commissioned by the department for Business, Innovation and Skills (BIS).² Only around half (53%) of respondents were confident that they would have sufficient security skills to manage their risks in the future. The PWC survey states: “There’s some evidence that skills shortages may be inhibiting what companies spend on security. Only 13% of respondents are

¹ Tracey Caldwell

² The path to becoming an information security manager (ISM). This shows previous roles held by people who subsequently become ISMs. Source: ‘Career Analysis into Cyber-security: New & Evolving Occupations’, E-Skills UK/Alderbridge.
very confident that they will be able to source sufficient security skills to enable them to manage their security risks. This compares with 20% who aren’t confident.” The skills shortage appears most acute in large organisations, where 9% are very confident versus 25% that aren’t confident.

Is there a skills crisis?

When does a shortage become a crisis? John Colley, managing director of (ISC)² EMEA believes his organisation’s 2013 Information Security Workforce Study clearly shows that there is a cybersecurity skills crisis.³ “Two thirds of C-level respondents view their security organisations as too few in number and more than 50% of respondents believe that staff expansion is justified: 71% of respondents reported feeling the strain of not enough staff in place,” he says. (ISC)² provides vendor-neutral education products, career services, and credentials to professionals in more than 135 countries. Its research shows that the top five skills that employers are looking for are a broad understanding of the security field (92%), communication skills (91%), technical knowledge (88%), understanding of the latest security threats (86%) and security policy formulation and application (75%). Colley adds: “Furthermore, infosecurity professionals recognise that they need to skill up in BYOD and cloud computing security.”

Skills in demand

E-skills interviews with 40 CISOs, who collectively manage over 6,100 cyber-security professionals, indicate that the top three in-demand skills areas are: information security architecture; risk management and compliance; and intelligence/threat analysis.

Anecdotally the people most in demand may be at the entry level and in the higher echelons of organisations. “The most significant issue, as I see it, will be on the high and low ends of the spectrum, in terms of applicable skills, as you will likely have people being put in place in entry level operational IT security jobs who simply do not have enough background to do the work to its fullest, and you will have people elevated into management positions sooner than they might merit based on sheer demand alone,” says Bernard Zelmans, general manager EMEA at FireMon. “As you can imagine, this will also make life harder on workers in mid-level positions as they will be the ones who have to pick up the slack.”

“The most significant shortage is among those workers directly responsible for doing the hands-on work necessary to defend networks and systems. This is because these are the most in-demand professionals out”

He adds: “The most significant shortage is among those workers directly responsible for doing the hands-on work necessary to defend networks and systems. This is because these are the most in-demand professionals out there and they must be workers who have considerable experience to do it well. There simply aren’t enough trained people out there right now which results in both a shortfall in qualified individuals and the use of inexperienced people when there’s no other choice. “These would include people such as network security administrators, remediation staff, vulnerability and compliance audit specialists and pen-testers. These are not entry level positions,
and even having had some certification or training, the lack of hands-on work experience is a huge challenge.”

Other industry players identify a number of additional gaps. Marc Vael, director of global IT membership body ISACA and managing director at Valuendo, pinpoints technical security configuration, security architecture, technical security maintenance and a need for ethical hackers for network and database and application security.

Joram Borenstein, vice president, NICE Actimize, says: “Currently there is high demand for forensic analysts who can help comprehend from a technical point of view what transpired when an infection or outbreak occurs, typically on end user’s laptops or other devices. There continues to be demand for those with broader skillsets, as well, such as the ability to prioritise and manage a workload queue of incidents for investigation, those familiar with compliance initiatives, and network analysts who can track and trace how infiltration and exfiltration might occur.”

Rob Stavrou, director at Northdoor, believes that organisations need security professionals with deep technical skills who know how to defend systems and organisations. “If you add to that the fast pace at which advanced malware and APTs are moving, it’s incredibly difficult to define what ‘effective’ cyber-security skills actually look like,” he says.

For small and medium businesses, in particular, which do not want or cannot afford to invest big budgets in their IT infrastructure, protection against cyber-attacks is a challenge. For many, the answer lies in partnering with an outsourced IT provider that has the specialist skills and experience needed to defend against cyber-criminals. Yet, as Stavrou points out, there are many companies that offer general security advice but there is a real shortage of specialist companies that can provide an in-depth and comprehensive service.

Why is there a shortage?

Catalin Cosoi, chief security strategist at Bitdefender, believes a major factor putting pressure on the availability of IT security professionals is the rapid development of IT itself. “You would have been hard-pressed to find an expert in the security of mobile devices a few years ago and they are still not all that common, in spite of the rising tide of BYOD policies.”

He adds: “The legislative environment is another obstacle, especially in the UK. The Computer Misuse Act of 1990 as amended by the Police and Justice Act of 2006 (section 37) makes developing, possessing and/or obtaining ‘articles for use in computer misuse offences’ a crime. The category includes such tools of the legitimate security professional as software disassemblers or network mappers. Of course, the law requires proof of intent, but relatively few people are willing to risk a trial just to get an education in an arcane IT field.”

Too few women

When E-skills UK engaged Alderbridge Consulting to undertake an analysis...
of intelligence covering the current recruitment landscape within cyber-security, one of its most striking findings was that men fill 86% of cyber-security roles, while women fill only 10% (there is no data for the remaining 4%).

“A lack of women interested in the sector reduces the pool of talented individuals that organisations can recruit from”

“The lack of female talent within cyber-security, as well as the wider IT sector, is a problem for a variety of reasons,” says E-skills’ Skidmore. “Firstly, a lack of women interested in the sector reduces the pool of talented individuals that organisations can recruit from. Secondly, there is evidence to suggest that organisations with a more even gender split perform better. For instance, the Credit Suisse Research Institute reports that over a period of six years, companies with a gender-diverse board outperformed male-only ones by 26%.”

E-skills is addressing this in a variety of ways. 135,000 girls in 3,800 schools have participated in its Computer Clubs for Girls (CC4G) since 2005. “These clubs highlight the exciting ways technology is used in music, sport and crime investigation, for example, and feature information security content. Some 88% of girls say they are more likely to consider further education or careers in technology as a result of taking part,” says Skidmore.

He adds: “We’re also developing entry routes into technology careers that are more attractive to women. For instance, our Information Technology Management for Business (ITMB) degree course instils a mix of technical and professional skills, with 34% of students being female – more than double the proportion on other IT courses.”

Bill Walker, security analyst and technical director at QA, the IT training company, says that, according to QA research, cyber-security is one of the least likely segments within Britain’s £81bn IT and telecoms sector to employ women. “Interestingly, in 2012, just 6.2% of over 2,500 people trained by QA in cyber-security were women. This data seems to reflect a worrying low number of women in the cyber-security profession. This figure is a third of the overall proportion of British women working in IT and telecoms, which already stands at a meagre 18%.”

“In 2012, just 6.2% of over 2,500 people trained by QA in cyber-security were women. This data seems to reflect a worrying low number of women in the cyber-security profession”

Things are not yet looking up. The number of women who took cyber-security training with QA during 2012 also declined in real terms by almost a fifth, down 19.5% compared to the figures for 2011. During the same period, the number of men taking cyber-security training more than doubled, increasing by 118% between 2011 and 2012.

Lysa Myers is a virus hunter for Intego, a Mac security software company. She believes the shortage in skilled cyber-security staff of both genders may be a cultural issue that could be addressed by more flexibility on the part of employers: “While there may be a technical skills shortage, I don’t believe it goes as far as a crisis. The bigger problem might be a mismatch between the expectations of employers and the needs of technically skilled employees,” she says. “I think, having many friends that are incredibly skilled in the area of information security, many of whom have been unemployed for a significant length of time purely for a lack of finding the right position, has definitely led to me seeing things differently. A surprising number of highly technologically forward-looking companies have very old fashioned views of co-location, for instance.”

She adds: “In order to attract and retain the best minds, and to get their best results, companies may need to adjust their expectations. This does not mean letting an employee run rampant, being unproductive or unresponsive, but a happy engineer can often work minor miracles when they’re allowed to get into their own zone.”

Myers believes a strongly supportive culture is essential in attracting top cyber-security staff: “It’s a never-ending task, as there will always be new holes and new attacks to deal with. The burn-out rate for security professionals is even higher than law enforcement officials, because of these factors. You have to have a very thick skin and a desire to ‘save the world’ that goes far beyond winning specific battles. But as a result, the security community is incredibly tight-knit. In much the same way soldiers in battle become like instant family, so too does the information security community. That closeness is what keeps a lot of us in this industry through even the roughest times.”

Tackling the shortage

James Lyne, director technology strategy at Sophos, identifies three major issues that contribute to the security skills shortage. The first is that cyber-security isn’t a clear or advertised career path.
“When was the last time a careers advisor at school said, ‘Have you thought about a career in cyber-security?’,” he says. “It’s a sadly infrequent occurrence. For many the path into the infosecurity profession is not clear at all and there isn’t a good understanding of the myriad different roles and what they might entail. As an industry, government and nation we need to do a better job of explaining that these jobs are interesting, rewarding and available even in the present times of financial difficulties.”

The second issue he identifies is that, in the UK, the curriculum is out of date and there isn’t a big enough pipeline of talent: “The scrapping of the GCSE IT curriculum and the 60% reduction in the number of people taking GCSE IT and A level since 2003 should be evidence enough that there is a significant issue in the development of talent through school years. Much like the engineering challenge reported a few years back, IT is often out of date by the time it is taught, given the pace of technology.”

The third issue, he believes, lies in the difficulty of junior security people getting the experience they need to progress to more senior jobs. “To tackle the skills shortage we need more people developing their experience, which means more internships, more junior roles with mentoring and more use of recognised certifications. As part of the UK Cyber-security Challenge, organisations like SANS are offering recognised certifications that demonstrate capability and at Sophos we’re trying to encourage more internships and development, though this has to be a broader national initiative to truly rectify the issue.”

The failure of the industry to attract young talent is a real issue. “Analysis of Alderbridge Consulting’s recruitment database shows that only 7% of information security professionals are under the age of 29, highlighting that we need to do more to showcase career opportunities in the sector and provide entry routes into them. We are doing this in a variety of ways,” says Skidmore.

“Firstly, by reforming the uninspiring ICT curriculum in secondary schools through our Behind the Screen project. This already provides industry-backed content on cyber-security at GCSE level, used by over 150 schools. We are now developing similar content at A level.

“Secondly, by seeking cyber-security employers to work with us on schools outreach, to provide teachers and careers advisors with a toolkit about the sector, and develop a bank of inspirational speakers and role models, particularly women, to discuss the exciting work they do.

“Thirdly, by developing the first ever nationally available, degree-level apprenticeships in cyber-security. With few security-specific undergraduate courses available, these will offer young people the opportunity to start their career, earn a salary and work towards globally-recognised qualifications.”

Employers, including QinetiQ, BT, IBM, Cassidian, CREST and Atos, are working with e-skills to develop the apprenticeships in cyber-security starting later this year.

“Employers, including QinetiQ, BT, IBM, Cassidian, CREST and Atos, are working with e-skills UK to develop the first ever nationally available, degree-level apprenticeships in cyber-security starting later this year”

Joanna Poplawska, co-founder of The Corporate IT Forum Education & Skills Commission, points out that in 2011 the Forum surveyed 66 of the UK’s largest IT user organisations and over a quarter cited security as an area of their business where they were experiencing a skills shortage. “The Commission believes the shortage needs to be addressed in schools now. Alarming is that we have seen a distinct lack of attention devoted to security and testing in the new computing curriculum,” she says.

She believes an interest in a career in cyber-security could be fostered at primary school. “In our submission to the Department for Education consultation, we called for the introduction of these elements at key stage 2, to introduce pupils to concepts including information and IT security, basic risk analysis, basic testing strategies and bugs.” Key stage 2 is age 7 to 11 in schools in England.

She warns: “There is no overnight solution, and it is going to take years and years to ensure the talent pipeline is at a stage that is fulfilling requirements. The 12 year olds making their subject choices now are going to form the next generation of IT skilled workforce and they need to be encouraged into careers in computing and STEM [Science Technology Engineering Maths]. This is why the Commission recommends that all schools should be required to ensure pupils have access to careers professionals with a STEM specialism and that the Government ensures that this requirement is funded adequately.”

IET initiative

There is no shortage of initiatives to address the cyber-security skills shortage through education. In June 2013 the Institution of Engineering and Technology launched the Cyber-security Skills Alliance with the BCS, The Institute of Information Security Professionals (IISP), E-skills UK and the Information Assurance Advisory Council (IAAC), to create a sponsorship scheme that will facilitate the granting of substantial bursaries for those studying masters-level degrees in cyber-security. The aim is to equip students with skills that they can apply in their current job, or to give them the opportunity to develop a career in a cyber-security role. The scheme is being launched through existing MSc courses at De Montfort University, Lancaster University, Plymouth University and University of Warwick.
Some observers warn against a situation where there are too many qualifications, leading to a plethora of qualified people all with different qualifications that are difficult for employers to compare. John Yeo, EMEA director at Trustwave, points out there appears to be no standards body, or professional ethics body for the cyber-security industry. “What we have is a large patchwork of ‘qualifications’ which, due to a lack of industry regulation, means there can be some very low barriers to entry for people proclaiming to be cyber-security experts. While this is not directly a cause of any shortage, it does make it difficult for employers to separate the wheat from the chaff.”

“What we have is a large patchwork of ‘qualifications’, which, due to a lack of industry regulation, means there can be some very low barriers to entry for people proclaiming to be cyber-security experts”

He calls for hands-on training: “While theory, concepts and research are a clearly important factor; practical professional experience is something we ourselves at Trustwave SpiderLabs value very greatly during the talent acquisition process, as well as a strong educational foundation. It would be prudent to ensure that educational institutions provide students with a core body of foundation knowledge combined with a sufficient level of practical, hands-on and industry experience.”

Too many certifications

E-skills’ Skidmore believes that it is up to the market to decide whether there are too many certifications: “However we are helping employers and individuals choose which ones are right for them via our new Cyber-security Learning Pathways.” The Pathways enable users to see what training and certifications are appropriate for specific job roles and levels of seniority.

Government initiatives to address the skills shortage, such as the EC Grand Coalition for ICT skills and the £7.5m government fund that will create two research centres to combat the growing threat of cyber-attacks as part of the UK National Cyber-security strategy, are welcome measures according to Mark Wiley, at training company Espion. “We also welcome reforms to work permits that remove the roadblocks and allow access to skilled workers outside the EU,” he says.

“Without doubt, when organisations commit budget to upskilling staff they are looking for the trust and assurance of globally recognised certifications,” he says. “Another highly sought after skill and one we’d recommend IT security professionals undertake is training to know the enemy. Courses like CEH [Certified Ethical Hacker] v8, which look through the eyes of the hacker to gain an insight into the insecurities, vulnerabilities and exploits that lie within your organisation’s systems, can further help firms to stay protected.”

Addressing shortfalls

Paul Somerville, professional services manager for expert data and security consultancy, Auriga, says: “The government’s strategy for cyber-security will certainly help in funding and addressing such shortfalls and skills gaps. Equally, initiatives such as the CESG Certified Professional scheme and government’s engagement with academia such as the Academic Centres of Excellence in Cyber-security Research will increase the UK’s academic capability in all fields of cyber-security. But the wider education system could also be improved upon by looking at how other competitive nations educate their youngsters in cyber-security.”

He adds: “Finally small businesses can review skills and look at appropriate training and education of staff to up-skill those with the right aptitude into cyber-security roles and these organisations could also make use of the Government’s Cyber-security Innovation Vouchers.”

The future

E-skills is urging employers to get involved in designing training for young people to make sure that skills needs are met in future. “We have already created two employer steering groups – one to guide our overall cyber-security skills strategy and another to develop degree-level apprenticeships in the field. Organisations involved include QinetiQ, BT, IBM, Cassidian, CREST and Atos, as well as SMEs from the Malvern Cyber-security Cluster,” says Skidmore. “But we want to hear from more organisations, particularly those who are keen to get involved in our schools outreach and curriculum development work, or help design apprenticeship programmes and hire new recruits through them.”

About the author

Tracey Caldwell is a freelance business technology writer who writes regularly on security issues. She is editor of Biometric Technology Today, also published by Elsevier.

References