WOMEN IN CYBER SECURITY

Ruth Massie *explores the shortage of women in this growing area and examines what can be done about the shortfall*

Take a group of 10 people working in the cyber security industry globally, and you'll find that only one of them will be a woman. The 2017 Frost & Sullivan report, *Women in Cybersecurity*, goes further in exposing the inequalities of the cyber security world. Surveying 19,000 information security professionals from 170 countries, the researchers found that men dominate all senior, board director and management positions. Women are stuck in entry-level positions. This is in a context where more women have a master's degree level qualification (51 percent) than men (45 percent). It doesn't add up.

A clear implication from the research is that cyber security – just like the wider universe of IT – involves a working culture that's unsympathetic to women. For example, 40 percent of women were found to give up on their jobs compared with fewer than 20 percent of men, having experienced problems in relation to opportunities for progression.

Just one in 10 people working in cyber security is female

This picture of dysfunction makes no sense for an industry struggling to attract enough skilled professionals to meet rapidly growing demand. There's an increased realisation that all businesses are now cyber businesses. It might be a small pizza takeaway outlet on the high street, but the pizzas are available through an app, so it's a cyber company. Digitisation of public services, transport systems, logistics and finance, means life in all developed nations operates in a cyber dimension, and a dimension open to cyber manipulation. Both policing and military activities have to be in a position to manage the new complexity of cyber crime and attacks, a world of threats that is growing and mutating at an unprecedented pace and on an unprecedented scale. But it's estimated that 1.8 million positions will be left unfilled internationally by 2022. The introduction of the UK's National Cyber Security Strategy is a reflection of the level of concern: schemes to position cyber security as a defined and attractive profession, for re-training IT workers, for more apprenticeships and a new professional body.

Attracting and retaining more women in cyber security isn't just an issue of increasing supplies of willing professionals. Cyber security needs the particular skills, qualities and insights that female recruits at all levels can deliver.

IDENTIFYING THE PROBLEM

A central problem to the development of cyber security as a profession has been that it continues to be seen as just another strand of IT: a technical discipline best undertaken and managed by technical people. Cyber security is more than that. It's where IT and all varieties of human behaviour and interactions come together. For organisations in particular, it's an issue of how all staff make use of digital technologies and all the forms of data involved, it's about the interplay between IT and each of the business functions, HR, finance, marketing. IT in the hands of everyone, not an esoteric activity that's best left for the initiated few. As consumers make more use of cyber security software at home – cyber crime levels were reported to have dipped in 2017 – but attacks on businesses are growing as criminals eye more profitable opportunities, making more use of malware, ransomware and Trojans. The National Cyber Security Centre reported that in the first three months of its existence there were 188 high-level attacks that demanded its intervention. Small and medium-sized businesses, with less investment in security, are also now seen as favoured targets.

There is a critical role for cyber security professionals in acting as the bridge between the two worlds of IT and general business management, to translate IT issues for managers and directors, to broaden out the CIO role, and make cyber security part of the everyday working culture, not the updating of software. Women are well placed to take on these interdisciplinary roles. In general, the women who do advance to more senior roles in IT have more of a variety of qualifications and backgrounds (in social sciences, humanities and management), while men, almost exclusively, have IT or engineering degrees. Women, typically, are recognised as having the softer skills needed to build relationships and awareness of the management issues involved and particular ways of working needed for cyber security. Other softer skills needed include adaptability and flexibility to deal with the pace of change, with high levels of ambiguity, in situations which can't always be controlled. Professionals need to be able to combine a level of technical knowledge with other forms of knowledge, of data protection and other laws.

DIVERSITY OF PERSPECTIVES

In terms of technical challenges and applications, diversity of perspectives are also important – for understanding human behaviours in the use and mis-use of digital technologies. Again, women in IT can bring insights that are more sensitive to the psychology of people and the personalities involved in the development of cyber attacks. What are their motivations, their likely targets, strengths and weaknesses, and therefore their likely next steps? Also, what are the factors and situations that will discourage people from taking part in cyber crime? Research since the nineties has highlighted how cyber crime appears almost entirely to be committed by men – one study, for example, suggested a ratio of one female hacker in 100 – and is a reflection of the male-dominated IT culture. But as cyber crime proliferates it will be increasingly important for the security services to also develop in sophistication, not just seeing it in terms of the black and white of coding and a purely technical response, but understanding, anticipating and countering operations devised and run by people. Perceptions of cyber criminals among the general public have been affected by media portrayals of harmless 'geeks', the cliché of young men in their bedrooms, when the reality is far more complex. The diversity of types of criminal activity online – extending from the more straightforward hacking of information, to pirating content, selling illegal products, online stalking and harassment, many of them being activities that are linked – make it necessary to have a much broader range of expertise. Gender stereotypes also mean that the fear of cyber crime, of being a victim, is also out of balance. Women playing a more active role would have a ripple effect in the wider population and help change the mindset of IT as a masculine threat.

THE OPPORTUNITIES FOR NEW ENTRANTS INTO THE WORLD OF CYBER SECURITY ARE BOUNDLESS

TIME FOR CHANGE

The need for a shift towards gender equality and a new culture for cyber security professionals is at the top of the National Cyber Security Centre's agenda. The Chief Executive, Ciaran Martin, has described the ongoing gender gap as "scandalous" and ensured a 50/50 balance in the senior leadership of NCSC. Current initiatives include working with private sector employers to offer first-job placements for female STEM graduates; introduce a new 'cyber

code of conduct' to help highlight the working culture issues and ensure women feel respected and treated equally; and ensuring women returning to technological roles after a career break receive mentoring and sponsorship.

DEVELOPING A CAREER

At Cranfield University we have a Cyber Masters programme that has 14 modules, and of these nine are run by women. There's been no conscious effort to redress the balance – it's happened organically, and more as a reflection of the variety of expertise and skills needed in the field. As part of a commitment to support the NCSC mission, a new

> THERE'S AN INCREASED REALISATION THAT ALL BUSINESSES ARE NOW CYBER BUSINESSES

Women as Cyber Leaders scholarship scheme has just been launched to encourage women to develop a senior career. The scholarship is worth £6,500 towards tuition fees for the MSc Cyber Defence and Information Assurance starting in October 2018. The programme is designed to develop professionals who can lead in a cyber environment, to effectively exploit the threats and opportunities of cyberspace at the organisational level, and focuses on understanding and articulating the executive-level responses to serious present, and emerging, threats in the information domain. Typically the participants on the programme – supported by the Cabinet Office and the Office of Cyber Security and Information Security – are from the Ministry of Defence, but increasingly are coming from other sectors such as telecoms, banking and insurance.

OPPORTUNITY KNOCKS

On the surface, the career opportunities for new entrants into cyber security are boundless. The skills shortage means salaries are high (and rose by 10 percent last year, well above the national average, according to recruitment consultants) and there's every chance of rapid progression. As an environment for the long term, however, the current situation isn't sustainable. There's too much dependency on older, senior – male – IT managers and consultants. And while there are growing numbers of degree courses, programmes and apprenticeships, there will continue to be obstacles, blockages and a waste of skills if the wider cultural issues aren't addressed. More diversity in the management and leadership of cyber security will be an essential factor in creating a profession with the character and energy capable of dealing with one of the greatest threats to global security ●

Ruth Massie is a Senior Lecturer in Cyber Governance Information and Decision Management at Cranfield University. Ruth previously worked as a Business Continuity Manager for Ernst & Young, Citigroup and Swiss Re. She was actively involved with London First and the National Counter Terrorism Security Office (NaCTSO) in developing the 'Expecting the Unexpected' business advice.

It's estimated that 1.8 million positions will be left unfilled internationally by 2022