The Daily Telegraph

SPECIAL REPORT

Thursday 18 February 2016

Careers in cybersecurity

KEEPING PACE WITH A CHANGING WORLD

The cybersecurity industry is growing at a dizzying rate. **William Ham Bevan** looks at the biggest developments, and finds out what they mean for job-hunters

GETTY/CBS PHOTO ARHIVE

Tools of the trade **Shows like CSI: Cyber are shining a spotlight on this booming sector**

Barely 20 years ago, cybersecurity was the preserve of a tiny number of highly specialised workers. Today, anyone considering it as a career is faced with a huge array of different roles, from penetration testing – where organisations hire a team to check whether their networks are susceptible to being hacked – to product development.

"We employ a wide variety of people," says Heath Davies, CEO of information security specialists Clearswift. "Just within our engineering division we have technical architects, developers, test engineers and technical authors, who put together the help manuals for our products. These are all jobs that only came into being recently."

There are still plenty of traditional security experts who look after firewalls and email. But an emerging group of people are focusing on things like cloud collaboration and social media.

Not all of the roles demand detailed knowledge of computer science. Increasingly, security is a strategic issue for companies, and this means there are opportunities for people with planning skills who can manage tasks such as carrying out risk assessments and developing contingency plans. Jobs that use behavioural analysis to predict threats, meanwhile, require a background in psychology.

On top of that, there are roles connected with data-protection legislation and ensuring that organisations are compliant with any relevant standards. For these, a background in law is valuable.

"The technical aspects are very important; but there are also non-technical parts of cybersecurity that are equally vital," says Prof Awais Rashid, director of Security-Lancaster, the specialist research centre on security science at Lancaster University. "Within my research team I have psychologists and sociologists, not just computer scientists. Security is all about how humans and technology intersect with each other."

Prof Tim Watson, director of WMG's Cyber Security Centre at the University of Warwick, agrees. "Whether you're a technical specialist, a behavioural scientist, a linguist or belong to one of the many other disciplines that are in demand in the sector, you should build your network and look out for suitable posts," he says.

Far from being backroom boffins, cybersecurity professionals often draw on communication skills. A penetration tester might be enormously technically skilled, but unless they're able to clearly present their findings, they're unlikely to progress.

"We need people whose expertise lies in working with people and organisations," says Chris Clinton, a security consultant at BAE Systems Applied Intelligence. "These experts in people are vital, as they work with businesses to improve their security policies and procedures as well as explain how the threat affects them."

Few sectors are as fast moving as cybersecurity, as new ways of using technology invariably bring with them new threats. Businesses are more connected than ever, with collaborative tools and social media changing working practices. This means it's often inappropriate simply to block access when a threat is detected; the challenge is to prevent access to sensitive data while still leaving valid business communications unhindered.

Likewise, as more and more real-world devices are connected to networks – the "internet of things" – the scope for attacks will increase, and this vulnerability is identified as a significant trend in BAE Systems' cybersecurity predictions for 2016.

Prof Rashid also believes that the near future will see threats against critical infrastructure gain prominence. "Eighteen months ago there were few people considering that power plants, water-treatment facilities, refineries and so on would face significant attacks," he explains. "But these infrastructures are connected to the internet in intricate ways, often designed at a time when cybersecurity was not a major concern."

Clearswift, meanwhile, predicts that the risks of ransomware (where someone infects your system, blocks it or encrypts the data and demands money for you to regain access) will continue to grow, targeting entire businesses.

With this proliferation of threats, the demand for cybersecurity professionals will only increase, and initiatives to raise awareness of the sector are being launched across the UK (see page 3). The number of courses and diplomas in cybersecurity is also rising, and a select few master's degrees have achieved the gold standard of accreditation by GCHQ.

However, these will only succeed if enough people take them up – and Chris Clinton of BAE Systems believes there are strong reasons to do so.

"I chose a career in this field because the work is extremely dynamic, and offers a high degree of job security," he says. "The skills shortage presents an issue for the industry, but it means there's a huge opportunity for people thinking about joining. The sector is only going to continue to expand and require more people – from all walks of life."