

The role of universities in addressing the demand for cyber security skills

Prof. Keith Martin
Director, Information Security Group
Royal Holloway, University of London

The adoption of the small word "cyber" has woken up the world to issues that many in the information security profession have been wrestling with for decades. And it's about time too. We have "cyber security strategies", "cyber security summits", "offices of cyber security" and a "cyber security skills crisis". Cyber security is of immense importance to everyone, and will only get increasingly so as the internet entwines our professional and personal lives.

What is increasingly clear from the stream of widely-reported incidents is that the provision of cyber security requires a "big picture" vision. Securing computer connections is of limited value if the data ends up on unprotected databases. Locking down hard drives is but a gesture if a copy exists on an unencrypted memory stick. The securest computer system in the world does not protect anyone from printed content being snapped by the telephoto lenses of the media.

Universities such as Royal Holloway are uniquely placed to provide a birds-eye view of the cyber security landscape. One of the fundamental differences between a higher education qualification and more targeted training is the focus on issues and appreciation, rather than short-term problem solving. It is of greater value to understand, for example, the principles and issues surrounding authentication than it is to be well-versed in the operation of a particular commercial product.

There are some worries about falling numbers of computing students in the light of demand for future cyber security professionals. This has potential to concern. However, from a cyber security perspective, I believe that there are good reasons not to panic and that there are opportunities to be explored.

It is important to appreciate that cyber security involves a wide range of skills. In the twenty years that Royal Holloway has been providing cyber security education programmes, we have educated almost 2000 professionals, many of whom were already well advanced in their career. We have seen, perhaps better than anyone, the diversity of routes that people enter the cyber security profession from, as well as the range of opportunities that they pursue after completion. This is a very healthy situation since cyber security is not a narrow field of specialism but is now a state of awareness with which everyone must engage.

And cyber security is cool. With this comes a tremendous opportunity to address any perceived skills gap head on. Initiatives such as the Cyber Security Challenge, which Royal Holloway has keenly supported, provide a vehicle not just to entice newcomers into the cyber security profession, but to reignite an interest in computing itself. There may well be a shortage of cyber security skills, but many of the vehicles to bridge it are already in place.