Is cyber security being taught correctly?

Students, Accademia and businesses all want different things from security. Dr Nigel Houlden, Dr Victoria Jackson and Dr Moustafa Haj Youssef ask whether trying to meet all these demands is the right approach.

There is currently an international shortage of graduates with the required skills in cyber security, whereby demand for these professionals is far outstripping supply. Looking ahead to the future, a recent World Economic Forum report stressed that technologies and expertise in encryption and cyber security particularly, are in high demand.

This is not just a question of education responding to what industry may or may not want, the drive of cyber security comes from governments.

How can we ensure that the skills required are taught? Could the use of national and international frameworks be of use?

Some research around the various frameworks and the role of national cybersecurity strategies on the improvement of cybersecurity education have already been published but more UK specific analysis is yet to be released.

It would seem obvious to fill the skills gap by recruiting and training degree apprentices. Working in the cyber industry while gaining the required skills and academic knowledge should be the ideal solution. However, is there a difference in perception between the trinity: education, business and the student.

The perception

If you've ever watched any thriller that involves cyber security or hacking (apart from *Mr Robot*), there is either an oversimplification or utter fantasy to what is being presented. And to be fair it probably needs to be, otherwise watching our intrepid hero saying: 'Don't worry the firewall is hardened, they'll never get in… And it has been tied down so hard you couldn't squeeze virtual tissue paper in between the system and the outside world' would be pretty boring.

Here in lies our perception issue, the student possibly has a view that could be unrealistic, a few keyboard strokes and voila! we've penetrated the Pentagon. The business, obviously, would like a return on investment. Many employers are realistic in their expectation;

however, many may not understand the complexities that underlie the security of their technology.

They would like their new apprentice to solve all of the technical issues, risk analysis, hardware security, software security, ensuring they are GDPR and PECR compliance.

Then there is the academic side. Many cyber degrees spawned from computer network degrees. This is a logical fit. But, what about human factors, the insider threat, the law and regulation, what about regulation GDPR, DORA, PECR, FOIA or NIS and many others?

This gives us a problem – no company should allow a new degree apprentice to secure their network, giving them the keys to the server room is unadvisable to say the least. We need to ask the question: does all of this belong in the area of computing? Academically speaking, should, law and regulation, risk and governance be taught by law and business schools? Should human factors be taught by psychologists?

Where to start

The problem of where to start comes from perception. The company wants the degree apprentice to be able to do something, the apprentice wants to do the fun stuff and the educator has to teach the building blocks. These three agendas aren't necessarily going to be met.

One possible way forward could be to teach policy: the ISO/IEC 27001 standard and Cyber Essentials Plus. This could be useful to the business, gives the academic a starting point and many degrees take this approach. But, will it engage the student who watched *Blackhat,* starring Chris Hemsworth?

What should be taught

If we do a Google search on 'what is cyber security?', we get around 1.7m results and, potentially, lots of different opinions. In truth, like many subjects, cyber security is many topics pulled together. Add to this, there are many different job roles. This all means, what should be taught becomes an even more problematic question.

There are frameworks like CyBok (the Cyber Security Body of Knowledge) which has 21 knowledge areas. These are grouped in to topics including: Human, organisational and regulatory aspects, attacks and defences, systems security, software and platform security and infrastructure security.

Many of these could be drawn together under a degree title, to form coherent subjects. However, any degree that attempted to cover all the above wouldn't have the depth to ensure the student (or degree apprentice) would have sufficient useful knowledge.

This problem is extended further if we consider industrial certifications like CompTIA, ISC2 or ISAC.

Add to this, from an apprentice or student perspective, which one is more valuable: an industry certificate (because you are already a practitioner) or a university degree at the undergraduate level?

Include the other dimension of 'what does an employer think is better for their business' and understanding what should be taught becomes a very complex question.

Asking a student, what do you want to be? Asking a business what do you need? Asking an academic what are you going to teach to fill the first two answers is trying to solve a three-dimensional problem in a two-dimensional space.

A more focused dialogue is needed, possibly working with business to create degree titles (and content) that fill the roles industry requires.

What about a degree in, say, HR or organisational behaviour? Would it be sensible to include modules related to topics relating to cyber security's human, organisational and regulatory aspects?

By doing so you are creating a wider knowledge of cyber security and integrating it within traditional subjects. This would make cyber security less technical but more appealing to students and businesses.

Could the cyber security skills shortage be filled, in part, by appropriately taught practitioners from other specialisms who have been taught aspects of the CyBok framework?