

SECURING A GOOD DEGREE?

How well are security degree courses preparing students for the real world? Steven Furnell investigates.

With the increasing recognition of security as an essential element of IT and information management, it is perhaps not surprising to see the topic gaining a corresponding recognition within academia. However, the topic can clearly be approached at different levels, with some merely giving a nod towards it within related modules, and others going far further with dedicated programmes. From the perspective of the profession, it is the latter route that is of particular interest, as graduates would reasonably be expected to emerge as appropriate recruits into security careers. With this in mind, this article examines some of the challenges posed by academic programmes, and considers what the security profession needs from academia.

SUPPLY AND DEMAND

There is no shortage of courses seeking to address the topic of security, as well as various related areas such as digital forensics and ethical hacking. Approximately a third of UK universities are now offering related programmes, and at the time of writing there are at least 39 institutions with three-year full-time degrees that explicitly name security and/or computer forensics in their course title. Moreover, many institutions offer several variations of their courses (e.g. computer security and forensics, computer security and networks, etc.), with the consequence that anyone searching for such programmes will find themselves with in excess of 85 titles on offer. And this is just the undergraduate degree programmes; looking at the Masters level reveals a range of further courses, some from the same institutions and some from other players (indeed, while a search suggests that roughly the same number of institutions are offering named MSc courses in security, only 23 of these are from places also offering a related undergraduate programme).

On one hand, this looks like rather positive news, as it clearly highlights security as an area that is seen to be both important and popular enough to attract candidates to study it in its own right. At the same time, however, there is an underlying concern that the establishment of some of the courses may have been motivated by the apparent market opportunity



rather than an established interest in the topic. Looking at the content in some cases creates the impression of more general computing courses that have been 'flavoured' with the inclusion of some security-related modules, with the overall programmes then being badged as security in an attempt to capitalise on the popularity of the topic. Although this could still be good from the perspective of raising the profile of the area in its own right, it is less certain that the resulting graduates will emerge in a strong position to contribute to the domain. In fact, from the topics being covered, students themselves would sometimes be hard-pushed to know that they were studying a security-specific course.

At the end of the day, there needs to be a tangible alignment between the title against which students were recruited and the skills that they emerge with when they graduate. However, whether this will actually be the case is significantly dependent upon the course content and the surrounding academic environment.

AN ETHICAL APPROACH?

Perhaps one of the more obvious scenarios in which the title risks being primarily used to attract attention and drive recruitment is when it starts to refer to media-friendly keywords rather than the discipline area involved. A good example here is the number of programmes that have sprung up under the heading of 'ethical hacking'. The ethos of such courses is generally based upon offering candidates an experience that helps them to think like the attackers they will be required to defend against. However, the underlying topic is basically security, and so in some cases the title is arguably more of a marketing ploy, playing on the media association with the word 'hacking'. Indeed, putting the term 'hacking' as a keyword in the course title was found to prompt a fair degree of media attention¹, and so it could be reasonably assumed that this fact was not lost on those courses that followed.

Aside from the arguments that could be made about 'ethical hacking' being a combination of mindset and techniques rather than an academic discipline, the related activities

...with a plethora of recognised professional certifications, employers might legitimately ask where an academic programme is expected to add value.



are just one fairly narrow aspect of a wider domain (see, for example, the relatively small subset of the IISP skills groups that would be encompassed if someone was a practitioner in these aspects alone), and so it is questionable whether organisations should actually look for someone who is only qualified in these areas. Of course, this concern might not matter so much if the title is just being used as a marketing hook on an otherwise substantial security programme. However, in some cases a look at the underlying content of the courses reveals that the topic itself forms a very minor part of the overall syllabus. For example, one undergraduate degree currently available in the UK offers just four core modules (80 credits) across the *whole* programme (i.e. 360 credits in total) that have security or hacking actually mentioned in the title, with none of these appearing in the first year of the programme. So, whether 'ethical hacking' warrants its prominence as the lead words in the course title, and whether it is justified in being presented as the basis of the qualification, is perhaps open to question.

Ethical hacking is not alone in spawning a variety of programmes; a similar pattern has also been seen with the emergence of courses targeting computer/digital forensics (with the course content and related capability base again appearing to be more credible in some places than others).

STRIKING THE BALANCE

The discussion above should not be taken to mean that ethical hacking courses are bad or that security-related programmes must be full of modules *entirely* about security. In fact, at the undergraduate level in particular, the latter could be just as bad as having a programme with too little security content, in the sense that it again undermines the potential to develop a holistic view. For example, an understanding of software, databases, business principles and the like will all go some way to ensuring that a would-be security professional is able to operate in a wider context, with an appreciation of the things that they are trying to protect. So, the crucial thing is actually to strike the right balance; the course needs to have enough direct security

content for the term to earn its place in the title, but enough non-security coverage to ensure that it also delivers a rounded professional who can relate to the other parts of the discipline in which they will be operating. So, as a rough rule of thumb for an undergraduate programme, it is suggested that the desirable level is for somewhere between a third and a half of the taught credits (plus any project work) to be focused around security. By contrast, a postgraduate programme would typically be expected to have a more focused responsibility towards the topic (on the basis that candidates could be expected to have established the wider context already through their prior studies). With this in mind, an MSc programme might reasonably be expected to devote at least three quarters of its taught credits towards developing specialism in the security-specific topics.

It is also relevant to consider what candidates (and subsequently employers) ought to be expecting from an academic qualification. As with other areas of computing, students are likely to have an insatiable appetite for lab-based activity. However, while this may come across as all they want, it is most definitely not all they need. Meanwhile, with a plethora of recognised professional certifications, employers might legitimately ask where an academic programme is expected to add value. What it clearly should not be expecting to do is simply mirror what the certifications are aiming to offer. The purpose ought to be to build a wider level of understanding, cultivating the mindset of security and where it fits in, rather than just the nature of the latest attacks and tools etc. As such, the combination of theory and practice is again an area where the balance has to be hit right.

Figure 1 illustrates where academic qualifications can most usefully fit in alongside other forms of security certificationⁱⁱ. At the bottom layer we have fairly focused training and practical certification (e.g. based around specific vendors and/or technologies), while the higher levels progressively head towards a more holistic view, addressing more of the wider discipline but guaranteeing less in terms of detailed operational expertise. All are valid (and indeed the most valuable professionals may hold examples from several

THE AUTHOR

Steven Furnell,
Centre for Security,
Communications and
Network Research,
University of Plymouth

levels), but the key is to recognise the role that each level should play. A named academic programme could reasonably be expected to lay the foundations across a large proportion of the IISP skills groups, perhaps also accenting the delivery to provide a higher level of competence in some specific target areas. However, it may still be no substitute for some of the lower-level technology or vendor-specific certifications, which ensure that someone has the hands-on skills to take things into the field.

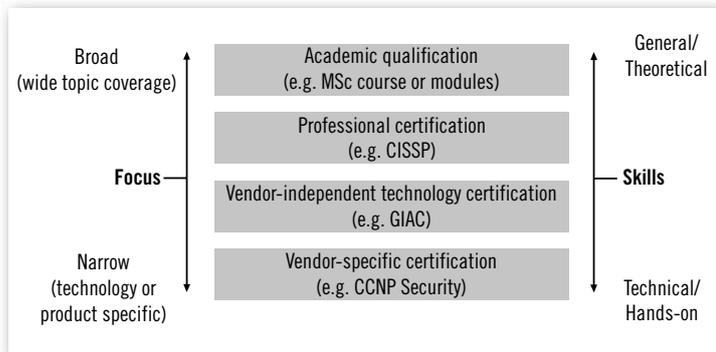


Figure 1: A taxonomy of security qualifications

It is also important for employers themselves to have appropriate expectations. An oft-expressed concern about IT courses in general is that they do not equip graduates with sufficient hands-on skills and experience to actually do the job in practice. However, it is here that we tread the line between providing education versus delivering training. It would be unreasonable to criticise a graduate just because they do not have specific experience in XYZ package. However, if their exposure to a practical topic has been entirely conceptual then they may well be of limited use to their first employer.

Aside from the content of the programme, another useful indicator would be where the topic fits into the academic mission and priority of the host institution or department. For example, is the course just one title amongst many topics offered, or does it fit into a wider profile of taught programmes, accompanying research, and external engagement? Indeed, while there are numerous UK universities offering security-related degrees in some form, there are fewer that could be said to offer a comprehensive academic portfolio, spanning undergraduate and postgraduate courses and related research activities. While offering the full range should by no means be seen as a prerequisite (or indeed a definitive indicator of underlying quality), it could at least be considered to be a useful secondary indicator, suggestive of a wider capability base. Similarly, one might reasonably think twice about an institution offering a security-themed BSc without any wider evidence of academic staff engagement in the discipline area.

CONCLUSIONS

Unlike some other aspects of IT, security is an area that simply will not work if it is done badly. So, if they are truly to serve the profession, the onus is upon academic institutions to ensure they are offering credible programmes that properly prepare their graduates for joining the wider community. Luckily, guidance is on hand for those that need it, in the form of materials such as the ISACA model curricula. Additionally, the IISP is increasing its own engagement in this field, with an Academic Partnership scheme and early moves towards accreditation of related courses. This, of course, will also help those looking to recruit into the profession, as they will have at least a baseline indication of how well a course is positioned to deliver against the skills they need.

References:

- i Shifrin, T. 2006. "Dundee to teach ethical hacking BSc", *ComputerWeekly.com*, 27 June 2006.
- ii Furnell, S. 2004. "Qualified to help: In search of the skills to ensure security", *Computer Fraud and Security*, December 2004. pp10-14.



MORE FULL MEMBERS OF THE INSTITUTE – M.INST.ISP

We would like to congratulate the following IISP members who have, since publication of our last *Pulse* magazine, achieved the Institute's professional accreditation, M.Inst.ISP. Well done.

In addition to now having full voting rights, and the ability to nominate directors to the Board of the IISP, we look forward to your further support in helping to develop the Institute, or contribute to its initiatives and working groups. Congratulations once again!

Stephen Bakewell

Robert Ball

Paul Bamford

Ian Begbie

Peter Bentley

Paul Boam

Damian Coombes

Paul Guest

Edward Hammond

Adam Harrison

Geraint Jowers

Mark Lewis

Martin McCormick

Phil Packman

Gary Pearson

Andy Preston

Colin Robbins

Keith Rogan

Paul Schwarzenberger

Nitin Shah

Neil Southwell

Nigel Strutt

Peter Thomas

Ralph Townshend

John Walsh

Colin Whawell

Dominic Wood