# Trainee cyber-criminals wanted to help solve skills shortage

December 3 2014, by Colin Mclean

Hacking can, and should, keep us on our toes. Credit: Alexandre Dulaunoy, CC BY-SA

The world is already short of computer security experts, but by 2017 that shortfall is going to have reached about two million. Criminal hackers cause damage running to billions of pounds every year – just look at the attack on Sony Pictures, leaking unreleased films onto the web and threatening the company's entire system. If we don't do something about this skills gap soon, the costs we bear are going to keep spiralling upwards and we will be increasingly vulnerable to cyber attacks.

This issue was raised by a panel of experts at the House of Lords recently, the National Audit Office has stated that the shortage of IT skills is hampering the UK's ability to protect itself, and Mark Weatherford – from the US Department of Homeland Security – has also stated that the lack of people with cyber security skills requires urgent attention as there simply aren't enough people to hire. With hacking and cybercrime being such hot topics at the moment – and with the demand for cybersecurity experts growing at 12 times the rate of the overall job market – how has this happened?

It's been suggested that the information security skills shortage stems from how few university leavers enter the field. But there are plenty of degree courses with relevant titles, so why aren't the graduates of these degrees not getting the jobs?

At the moment, the blame game is in operation: industry blames academia for being too theoretical, and academia blames industry for wanting something different from what they provide. This isn't getting us anywhere, but there are a few changes that could make a difference.

## Thinking like criminals

Courses need to be more vocational, something that unfortunately many academics and research funding organisations look askance at. But it's what's made our ethical hacking degree so successful: students don't just study theory, which of course is important, but conduct practical operations in a closed computer network lab, where the course focuses on getting the students to think practically and creatively in developing their experimentation skills. They need to learn to think how hackers think. We get them to look for a system's vulnerabilities, and to try and exploit any weaknesses they find by using their practical programming skills to test things out.

Although it might seem a bit unusual to breed a criminal mindset like this, the most effective way to build secure computer systems is to understand how you can break into them.

## Making connections

As well as working on practical tasks in the lab, students need placements at some of the country's top security firms. In fact close links with industry is key, as that way universities can learn from companies what skills are needed so that courses can adapt to provide graduates with exactly what they'll need to succeed.

We desperately need more of these relationships – it's no good having companies asking universities for their best graduates if they don't tell universities what it is they need these graduates to be able to do.

But this transfer of knowledge needs to go further. Students need to hear from industry representatives about the industry. It's equally important that our students and graduates go back to their schools and talk about what they're doing. This opens they eyes of pupils to what the industry might hold for them, and offers a bit of inspiration for pupils and their teachers.

Historically, computer science taught at school has focused on using applications – learning packages like Microsoft Word, Excel or Access, without delving much into the underlying operating system or hardware technology that makes them possible. Some of today's pupils have no idea about the sorts of things that computer science incorporates, nor what computers are capable of. But mention "hacking" and they sit up and take notice.

Perhaps there is a certain amount of nervousness about the sort of skills computer security courses must necessarily teach. But there is no security through obscurity – we have to teach the routes and mechanisms of attack in order to defend against those that would use them against us.

*This story is published courtesy of* The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Trainee cyber-criminals wanted to help solve skills shortage (2014, December 3) retrieved 27 April 2024 from https://phys.org/news/2014-12-trainee-cyber-criminals-skills-shortage.html