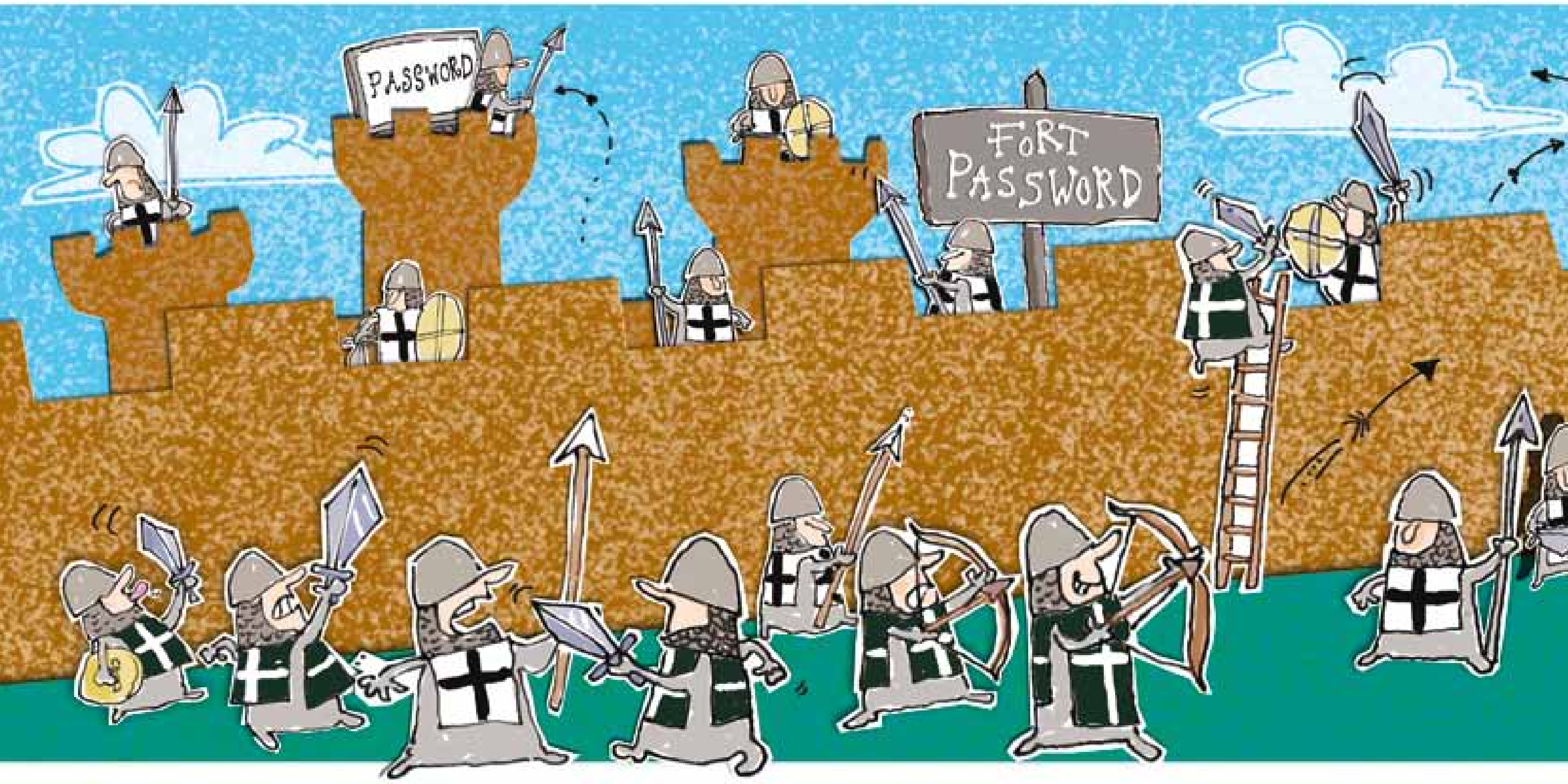


Securing the defences

Security of IT systems is a major issue in a world where they are becoming more and more ubiquitous. One way to test defences is by launching your own 'friendly attack' – employing penetration testers or ethical hackers to find any potential weak spots.

In autumn 2010, an 'ethical hacking' experiment conducted in six cities across the UK showed that almost half of private Wi-Fi networks could be hacked in less than five seconds, even if they were password-protected. A report published around the same time by internet security and anti-virus specialist Norton found that more than half of UK adult internet users had been the victim of a cybercrime at some point.

In the corporate world, a cyber security monitor report by BAE Systems found that over 80 per cent of companies believed that cyber criminals were innovating at a quicker pace than their security measures.

IT security issues featured big in 2010 – from the Stuxnet worm to 'hacktivism' in the wake of the arrest of WikiLeak's founder Julian Assange, to scares about data leakage on Facebook. In January this year, the Organization for Economic Cooperation and Development (OECD) published a study that found that attacks on computer systems now have the potential to cause global catastrophes, though only in combination with another disaster.

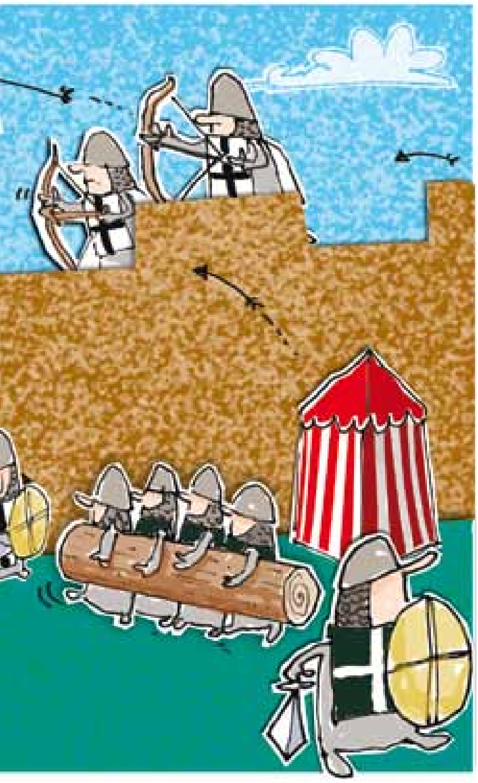
In the face of these 'scares', it is not surprising that the demand for IT security specialists is growing at a rapid pace. 'We have seen a tremendous surge in information security certified training requirements,' says Jay Bavisi, President of International Council of E-Commerce Consultants (EC-Council), an organisation that offers, among others, CEH, the Certified Ethical Hacker certification.

With the rate of cyber attacks doubling each year, IT security has become a valuable profession

'White hats'

One such specialist is the 'ethical hacker' – another name for what is also known as penetration tester (note that there has been much debate on whether the term 'ethical hacker' is appropriate, with some claiming that it is a contradiction in terms – in this article, the terms will be used interchangeably). With the rate of cyber attacks doubling every year, IT security has become a valuable profession, and many in the role of ethical hacker now demand a six-figure salary.

An ethical hacker is usually someone who is employed by an organisation and can be trusted to penetrate networks and/or computer systems using the same methods as a hacker would. The purpose is to find, and then fix, computer



security vulnerabilities. While illegal hacking is a crime in most countries, penetration testing or hacking done by request of the owner of the targeted system or network is not.

Ethical hacking in this sense came about in the 1970s, when the US government started using groups of experts to hack its own computer systems, and then became increasingly widespread outside the government and technology sectors. An ethical hackers is sometimes also called a 'white', a term that comes from old Western movies, where the 'good guy' wore a white hat and the 'bad guy' wore a black hat.

Risk detection

While there is growing awareness of the threats of cybercrime, ignorance or maybe carelessness regarding security issues still seem to pervade both the world of private and corporate IT. This is shown in the BAE Systems report referred to above, which also found that companies were still confident about the traditional tools they used, such as firewalls, anti-virus programs and

A report found that over 80 per cent of companies believed that cyber criminals were innovating at a quicker pace than their security measures

Certifications

The Council of Registered Ethical Security Testers (CREST) is a non-profit association created to provide recognised standards and professionalism for the penetration testing industry.

For organisations, CREST provides a provable validation of security testing methodologies and practices, aiding with client engagement and procurement processes and proving that the member company is able to provide testing services to the CREST standard. It offers three certifications: CREST Registered Tester, CREST Certified Tester (Infrastructure) and CREST Certified Tester (Web Applications). It also certifies companies.
www.crest-approved.org

The Information Assurance Certification Review Board (IACRB) manages a penetration testing certification known as the Certified Penetration Tester (CPT). The CPT requires that the exam candidate pass a traditional multiple choice exam, as well as pass a practical exam that requires the candidate to perform a penetration test against live servers.
www.iacertification.org

SANS provides a wide range of computer security training arena leading to a number of SANS qualifications. In 1999, SANS founded GIAC, the Global Information Assurance Certification, which, according to SANS, has been undertaken by over 20,000 members to date. Two of the GIAC certifications are penetration testing specific: the GIAC Certified Penetration Tester (GPEN) certification and the GIAC Web Application Penetration Tester (GWAPT) certification.
www.giac.org

Offensive Security offers an ethical hacking certification (Offensive Security Certified Professional). The OSCP is a real-life penetration testing certification, requiring holders to successfully attack and penetrate various live machines in a safe lab environment. Upon completion of the course students become eligible to take a certification challenge, which has to be completed in 24 hours. Documentation must include procedures used and proof of successful penetration including special marker files.
www.offensive-security.com

The Tiger Scheme offers two certifications: the first is Qualified Security Tester (QST), an entry-level qualification that is obtained after successfully passing a written examination set by the Examining Body or by submitting evidence of a recognised qualification (e.g. certain MSc courses). The second is the Senior Security Tester (SST), which requires the candidate to pass a practical examination demonstrating network security vulnerability analysis skills and to successfully pass an interview in order to demonstrate both their understanding and their ability to communicate their findings.
www.tigerscheme.org

The International Council of E-Commerce consultants certifies individuals in various e-business and information security skills. These include the certified ethical hacker course, computer hacking forensics investigator programme, licensed penetration tester programme and various other.
www.eccouncil.org

web filters. The report noted that 'such a high degree of confidence in existing defence systems was surprising', adding that 'it suggests that the reality and impact of the threats are not visible to business or that attacks are already happening below the radar of their traditional defences.'

Robert Chapman, CEO of Firebrand Training, which has been running Certified Ethical Hacker (CEH) courses for several years now, sees the same worrying signs: 'Firebrand has trained hundreds of ethical hackers over the past decade. However, major companies – and indeed individuals – still refuse to see the very real threat of cybercrime. The biggest concern is that hackers can threaten national security, and cripple major organisations. A company is only as strong as its weakest link, and if its employees are not aware of the potential pitfalls, that company could be destroyed with one moment of carelessness.'

Ensuring ethics

As ethical hacking can easily reveal sensitive information about a company, many security firms take care to show that all their employees adhere to a strict ethical code, and there are a number of professional and government certifications that vouch for a company's trustworthiness and conformance to industry best practice (see box out).

'The role of an ethical hacker comes with responsibility,' stresses Robert. 'Before we begin our five-day course, every student must sign an agreement to ensure that they don't use their new skills illegally.' Only once they have signed the agreement form do students receive the course pack, which contains, among other things, manuals, DVDs with self-study material and a large selection of tools. The second module of the course itself then covers hacking laws in the UK, the US, in Europe and various other countries.

Every student must sign an agreement to ensure that they don't use their new skills illegally

Robert Chapman, Firebrand Training

Certifying skills

Ethical hacking certification programmes aim to equip people with the ability to understand and know how to look for the weaknesses and vulnerabilities in target systems, using the same knowledge and tools as malicious hackers. Much is based on offering students practical experience in a hands-on environment where they can scan, test, hack and secure their own systems.

Mark Rouse, Director at FTI Consulting, who took the CEH course with Firebrand Training, found one of the most interesting elements of the course was discovering how readily available hacking tools were. 'The reason I took the qualification was to get a comprehensive grounding and understanding of the different tools and techniques that could be used by a fraudster to hack a corporate database system,' he says. 'Up until then, my primary focus was in using technology and techniques to uncover the hidden and usual patterns, relationships and anomalies in data that are symptomatic of potential fraud. Studying for the certification has allowed me to explore a further avenue of hi-tech fraud investigation, that of database intrusion and compromise detection.'

Others look at certification as a stepping stone in their careers development. Scott Dougherty, for example, decided to take the CEH course with Firebrand as part of his career goal of working in the computer security field. 'I took a number of certification courses from 7Safe, and during these courses I met various people who had done the CEH course and they commented how their employer had specified this course as a prerequisite for security jobs,' Scott explains. 'The other qualification that was mentioned was CISSP.'

'I found the whole experience very rewarding,' he adds. 'There was a lot of information to take in and a lot of tools to get familiar with. The breadth of the tools presented allowed me to refine my "toolkit" to be used in penetration testing.'