Cyber and information security

D 08 November 2023

Protecting computer systems and the information they hold from threats is vitally important. The number of jobs concerned with cyber and information security is increasing year on year. Entry to this area of work is possible for those with GCSEs (or equivalent qualifications), right through to postgraduates.

Cyber threats

Breaches of information security often hit the headlines, particularly when they affect well-known businesses such as banks or internet service providers. Cyber and information security breaches are becoming more common, so security has become an increasingly urgent issue. Legislation puts even more onus on organisations to safeguard personal data. To help reduce the security risk, the National Cyber Security Centre (NCSC) provides advice and support to cyber security professionals, businesses and other organisations.

Just consider how dependent we are on computer networks.

- We store information on our own devices as well as on data storage 'cloud' systems.
- Connectivity (sometimes referred to as 'the internet of things' or 'IoT') allows us to interact with our home heating, music and security systems, for instance, through the web.
- Businesses such as banks, retailers, energy suppliers, transport operators and so on depend on their computer systems in order to operate.
- Customers need to be protected when using online banking and contactless technology.
- Central government, local authorities and public services, such as the NHS, rely on computer systems to deliver their services, keep the country running and keep people safe.

Cyber and information security threats, such as the following, can have serious implications:

- malicious interference from computer hacking and viruses that corrupt computer systems
- threats to the confidentiality of data held electronically - including personal data that may be stolen and used for identity theft, and sensitive information held by organisations
- fake websites and 'phishing' emails set up with the intention of gaining customer information or stealing their money.

Cyber crime is widely considered to be the biggest threat to organisations and profits, and to personal data and finances. People from within or outside an organisation may be:

- criminals who want to benefit financially; online fraud is now one of the most common crimes
- spies who are involved in espionage (e.g. for business competitors, protest groups, political parties or even foreign governments)
- terrorist groups, whose aim may be to cause major disruption in order to undermine society or try to influence governments to take certain actions
- individuals working alone, who seek to invade computer systems for other reasons.

The work

New careers in cyber and information security have emerged in recent years and there is now a wide range of job roles. Employers in every organisation - business, industry, not-for-profit and public sector - need staff with cyber security skills. Employment opportunities are also available with tech companies, particularly in independent consultancies. Large organisations may employ a team of specialist staff responsible for cyber and information security, while in smaller organisations it may be the responsibility of one person, perhaps with advice and support from specialist consultants.

The main broad areas of work with examples of job titles are given below, but be aware that titles vary from employer to employer, and roles and responsibilities often overlap.

- *Information security management:* an **information security manager** or **chief information security officer (CISO)** takes responsibility for an organisation's information security strategy. They implement and oversee policies relating to matters such as authorised access to systems and data, and ensure compliance with legal and regulatory requirements. In the event of attack, they take responsibility for continuity of business planning and may manage a team of cyber security specialists.
- *Risk analysis:* **information security analysts**, **risk analysts**, **cyber intrusion/security analysts** and **secure/network operations centre analysts** identify potential security threats and assess their relative impact on the organisation's operations. They advise senior management and/or escalate issues to incident response staff.
- *Technical roles:* **security software developers**, **security architects**, **information security engineers**, **cyber security technicians/technologists**, **security administrators** - these are the various jobs concerned with designing, developing, installing, maintaining and upgrading information security systems, e.g. through firewalls, biometric scanning and multi-factor authentication. Those in analyst and technical roles need to keep up to date with the latest malicious software, in order to make sure that their organisation's systems are suitably protected.
- *Testers:* **penetration (pen) testers** assess the security of their organisation's systems, in order to find any areas of vulnerability. They have to think, and act, like computer hackers. This area of work is sometimes called **ethical hacking**, although pen testing is generally more targeted at finding problems with specific systems.
- *Forensics:* **computer forensic investigators** or **computer forensic analysts** are concerned with cyber crime and intelligence. They analyse computer systems to identify evidence of cyber crime, and collect and record evidence that may be used in court, in the event of a prosecution. For more information, see the leaflet on *Forensics* .
- *Other areas of work:* **information security consultants** provide advisory services to clients to help them develop and manage cyber security systems. **Trainers** (who may be known by a range of titles) ensure that members of staff are aware of the importance of security measures and that they know how to comply with security procedures.

What it takes

For cyber and information security work you need:

- a logical and analytical mind
- excellent problem-solving skills
- the ability to work well in a team
- to be able to pay attention to detail and work methodically
- persistence and patience
- to keep up to date with technological developments and adapt to change
- good communication skills
- the ability to work under pressure and to deadlines
- a respect for confidential information
- a sound understanding of organisational/business needs.

Entry and training

Entry to cyber and information security work is mainly at graduate level, although there are opportunities to start with GCSEs, A levels or equivalent qualifications and train in the workplace (see below).

Although information is given below about education and training in cyber and information security, for details on more general computing courses etc at various levels, refer to the leaflet *Digital careers - an introduction to the work and training*.

Higher education

There is a range of full-time, broad-based computer science **degree, HNC/D and foundation degree courses** that can provide a suitable background for cyber and information security work. There are also more specialist higher education courses, such as those in cyber security, digital forensics and ethical hacking. Some degree courses are offered on a **sandwich** basis, incorporating a year with an employer as part of the course.

Postgraduate courses in cyber security and related subjects are available. These are usually aimed at those with a first degree in computing or a related subject, or equivalent experience/professional qualifications.

GCHQ offers **CyberFirst Bursaries**. Successful students (who must have an offer of a degree course place - any subject is acceptable - or who have already started their undergraduate degree) receive £4,000 of financial support per year plus a summer placement. Find out more at: www.gchq-careers.co.uk/cyberfirst/university-bursary.html.

When choosing a higher education course, make sure you are aware of the exact content. Find out about employer links, facilities, the destinations of past students etc. Some courses are certified by the NCSC; see: www.ncsc.gov.uk/information/ncsc-certified-degrees.

Training in the workplace

A number of employers run **graduate training schemes**. Some take graduates of any discipline, but others require people with degrees in computing or other relevant subjects.

Apprenticeships can offer structured training with an employer. Relevant programmes in England include:

- level 3 for cyber security technicians
- level 4 for cyber security technologists with specialisms for cyber security engineers, cyber risk analysts and in cyber defence and response
- Degree Apprenticeships for cyber security technical professionals (level 6)
- Degree Apprenticeships at levels 6 and 7 (masters level - for which you are likely to need a relevant first degree) for digital and technology solutions professionals/specialists; these have specialisms for cyber security specialists.

In Wales, relevant Apprenticeships include levels 3 and 4 (Higher Apprenticeships) in information security; these can provide training in a range of roles including network security and pen testing. Also, the digital Degree Apprenticeship includes a pathway in cyber security management.

There are no set entry qualifications for Apprenticeships; each employer decides on their own criteria. However, entrants are likely to need some GCSEs at grades 9-4/A*-C (including English and maths), or equivalent, for an Apprenticeship at level 3, and A levels (or equivalent qualifications/relevant experience) for Higher and Degree Apprenticeships. To find out more about Apprenticeships, see:
www.apprenticeships.gov.uk
www.careerswales.gov.wales

Once employed in cyber and information security you need to keep your knowledge up to date, as technology changes at a rapid pace, and those who carry out cyber attacks find new ways to breach security systems. There are various **professional certification and qualification schemes**, e.g. the NCSC Certified Professional Scheme (CPS) - see: www.ncsc.gov.uk/information/about-certified-professional-scheme.

CREST (see under Further Information) offers a range of professional qualifications for those involved in assessing and testing security systems, and responding to security breaches. CREST also accredits training courses offered by a range of providers.

Some starting points...

To make yourself as employable as possible, get as much relevant experience as you can. For example, you can take part in online competitions, attend hack events and industry conferences, and get work experience (e.g. through a sandwich course, holiday job or internship).

A free, online **introduction to cyber security course** has been developed by The Open University, with accreditation by the **Chartered Institute of Information Security (CIISec)** and support from the Government's National Cyber Security Programme. The course takes three hours a week over an eight-week period. There are no set entry requirements. The course could be useful in your everyday life, if you're new to this area of work, or as a taster to see whether or not a career in this area would interest you. Find out more at: www.futurelearn.com/courses/introduction-to-cyber-security.

After taking GCSEs, the **Cyber Extended Project Qualification**, developed by a consortium of partners and accredited by City & Guilds, could be useful. This is an online qualification, equivalent to an AS level (attracting UCAS Tariff points), and can be taken through schools/colleges or independently. For details, view: https://cyberepq.org.uk.

CyberFirst, established by NCSC, offers a range of initiatives. For example, it runs the CyberFirst Girls Competition and a range of short courses for young people (including a residential course for 16- to 17-year-olds). You can find out more at: www.ncsc.gov.uk/cyberfirst.

Adults: *People who already have skills in other areas of computing may be able to move into cyber and information security.*

Prospects and pay

Severe skill shortages in cyber and information security have been reported worldwide, so there are good opportunities for those entering this area of work. Government research has found that in the UK in 2023, 50% of all businesses were experiencing basic cyber security skill gaps and 33% more advanced skills gaps.

With experience, promotion, e.g. to information security manager or CISO, may be possible. Those with suitable experience may choose to become self-employed consultants. Some cyber and information security experts work in research and/or teaching at universities and other institutions.

There are no set pay scales in cyber and information security. As a guide, graduate starting salaries are in the region of £20-30,000. Pay can rise up to £60,000 for those in more responsible positions. In leadership roles and areas of work where skills are in particular demand, salaries can reach £80,000 or higher.

Further Information

Chartered Institute of Information Security (CIISec) - offers membership for individuals and organisations, runs masterclasses, accredits training courses, including in cyber security awareness, and risk and incident management, and offers routes to Certified Cyber Professional (CCP):
www.ciisec.org

CREST (UK) - a not-for-profit organisation that represents the technical information security market. Offers membership, certifications and careers resources - see:
www.crest-approved.org

Cyber Security Challenge UK - find out about career opportunities and various learning programmes, and view resources etc, at:
https://cybersecuritychallenge.org.uk

UK Cyber Security Council - a new organisation set up to address skill shortages, standardise career paths and ensure a code of ethics is followed by those working in cyber security.
www.ukcybersecuritycouncil.org.uk
View their career pathways framework (with links to various career profiles) here:
www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework

Job vacancies can be found through the websites of general recruitment agencies, professional bodies and potential employers, and on specialist recruitment sites such as:

- www.itsecurityjobs.co.uk
- www.cybersecurityjobsite.com
- www.cybersecurityjobs.net

Related Leaflets

AB 02 Specialist careers in the Civil Service (includes security and intelligence services work)
D 01 Digital careers - an introduction to the work and training
D 02 Tech and digital support

D 05 Data analysis and management
D 06 Software design and development
D 09 Tech and digital management
D 12 AI and machine learning
D 13 Careers in digital systems
TD 12 Forensics (includes digital forensics)
UG 02 Police work
UK 01 Security work
UK 04 Disaster management and relief

© Copyright 2024. All rights reserved - Adviza Partnership