Cyber security analysts help to protect an organisation by employing a range of technologies and processes to prevent, detect and manage cyber threats. This can include protection of computers, data, networks and programmes.

Broadly, you can work in one of the following areas:

* consulting, offering advisory services to clients
* working to protect the security of the organisation you work for.

Job titles vary and may include information security analyst, security analyst, information security consultant, security operations centre (SOC) analyst and cyber intelligence analyst.

## Responsibilities

As a cyber security analyst, you'll need to:

* keep up to date with the latest security and technology developments
* research/evaluate emerging cyber security threats and ways to manage them
* plan for disaster recovery in the event of any security breaches
* monitor for attacks, intrusions and unusual, unauthorised or illegal activity
* test and evaluate security products
* design new security systems or upgrade existing ones
* use advanced analytic tools to determine emerging threat patterns and vulnerabilities
* engage in 'ethical hacking', for example, simulating security breaches
* identify potential weaknesses and implement measures, such as firewalls and encryption
* investigate security alerts and provide incident response
* monitor identity and access management, including monitoring for abuse of permissions by authorised system users
* liaise with stakeholders in relation to cyber security issues and provide future recommendations
* generate reports for both technical and non-technical staff and stakeholders
* maintain an information security risk register and assist with internal and external audits relating to information security
* monitor and respond to 'phishing' emails and 'pharming' activity
* assist with the creation, maintenance and delivery of cyber security awareness training for colleagues
* give advice and guidance to staff on issues such as spam and unwanted or malicious emails.

## Qualifications

It's possible to enter the cyber security profession without a degree by starting in an entry-level IT position. You could then work your way up to a cyber security role.

You could undertake an apprenticeship in cyber security, where you'd combine employment and study to work towards a recognised qualification.

Many employers recruiting for a graduate position require, or prefer, a degree in a science, technology, engineering or mathematics (STEM) subject. Exact requirements vary between employers. More relevant degree subjects include:

* cyber/information/network security
* computer science
* software/electrical/network engineering
* mathematics
* physics
* other IT/security/network-related degrees.

## Skills

You'll need to have:

* a passion for cyber security and a keen interest in IT
* excellent IT skills, including knowledge of computer networks, operating systems, software, hardware and security
* an understanding of the cyber security risks associated with various technologies and ways to manage them
* a good working knowledge of various security technologies such as network and application firewalls, host intrusion prevention and anti-virus
* the ability to work as part of a team and to build strong relationships with staff and other relevant individuals
* verbal communication skills, including presentation skills, with an ability to communicate with a range of technical and non-technical team members and other relevant individuals
* written communication skills, for example to write technical reports
* time-management and organisational skills to manage a variety of tasks, prioritise workload and meet deadlines
* excellent attention to detail, analytical skills and an ability to analyse complex technical information in order to identify patterns and trends
* an ability to work under pressure, particularly when dealing with threats and at times of high demand.

## Professional development

Once you're working in the field, it's important to keep up to date with developments. You may be able to access industry information, events and networking opportunities through, for example:

* [BCS](https://www.bcs.org/)
* [IISP](https://www.iisp.org/)
* [Information Systems Security Association (ISSA)](https://issa.site-ym.com/page/AboutISSA?)

Some employers, such as those offering graduate training schemes, may fund you to complete an MSc in information/cyber security while you're on the programme.

A part of GCHQ, NCSC lists bodies which they have certified to assess information assurance professionals. The [GCHQ Certified Training (GCT)](https://www.ncsc.gov.uk/scheme/gchq-certified-training) scheme offers courses at different levels: an 'awareness' level for those new to cyber security and an 'application' level which is more in-depth.

There are also various industry-related qualifications, such as:

* Systems Security Certified Practitioner (SSCP) - an entry-level, IT certification for those with at least one year of experience.
* The Certified Professional (CCP) scheme - the UK government's approved standard of competence for cyber security professionals. The scheme also provides those working in cyber security with a clearly defined career development path. There are different levels you can apply to - practitioner (entry level), senior practitioner and lead practitioner.
* Certified Information System Security Professional (CISSP) - you'll typically need at least four years of experience for this.

For those wanting to develop leadership, management and supervisory capabilities, there are a number of different certifications. These include the Certified Information Security Manager (CISM) for practitioners with five years of relevant work experience.

Other relevant courses include Certified Ethical Hacker (CEH), Cloud Security, Cyber Incident, Planning and Response (CIPR) and General Data Protection Regulation (GDPR) awareness.

Cyber security consultants can apply for the NCSC's Certified Consultancy scheme to receive certification. CCP certification is currently a prerequisite for this.

## Career prospects

Cyber security is a fast-growing field and there is currently a skills shortage. Career prospects are good for people with the right combination of skills and experience.

You'll typically start in an entry-level or junior cyber security role. After building up several years of experience you could progress into roles such as senior cyber security analyst or consultant.

After significant experience in the field, you may be able to progress into higher level leadership and managerial roles, eventually progressing to become a director or head of cyber security. Achieving relevant certifications is helpful for your development and progression as many employers specify these as role requirements.

Self-employment is an option, but most people first gain experience in the field. You could set up a cyber security company or work as an independent cyber security consultant.