Cyber security analyst

Cyber security analysts help to protect an organisation by employing a range of technologies and processes to prevent, detect and manage cyber threats

As a cyber security analyst, you'll monitor networks and systems, detect security threats ('events'), analyse and assess alarms, and report on threats, intrusion attempts and false alarms, either resolving them or escalating them, depending on the severity.

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 vulnerabilities and ways to manage them
- plan for disaster recovery and create contingency plans in the event of any security breaches
- monitor for attacks, intrusions and unusual, unauthorised or illegal activity
- test and evaluate security products and check suppliers' certification, compliance and accreditation
- 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 using incident handling methodologies and best practices
- monitor and respond to common cyber threats such as 'phishing' emails, 'pharming' activity, malware and ransomware

- 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
- record all findings, actions taken and lessons learned following an incident to strengthen future responses
- generate incident reports for both technical and non-technical staff and stakeholders
- review and improve security processes
- maintain an information security risk register and assist with internal and external audits relating to information security
- promote a culture of security amongst colleagues and other stakeholders and support wider security initiatives
- 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.

Salary

- Salaries for cyber security analysts with one to three years' experience typically range from £37,500 to £52,500.
- Experienced cyber security analysts with four to six years' experience can earn between £47,500 and £60,000, rising to between £65,000 and £80,000 for senior analysts with seven to nine years' experience.
- In higher-level managerial or leadership roles, you may receive salaries ranging from around £72,500 to in excess of £100,000.

You'll usually receive a range of employee benefits that may include a bonus, company pension scheme, private medical insurance, gym membership, and sponsored training and development opportunities.

Income data from Cybershark Recruitment. Figures are intended as a guide only.

Working hours

Working hours are typically 35 to 40 hours per week, Monday to Friday. You may need to work outside of 9am until 5pm depending on projects and the specific nature of the work.

Some companies may require you to work on a shift basis, which can include evenings, nights and weekends. You may need to work as part of a 24/7 call-out rota, to allow for quick responses to cyber security incidents.

Some companies offer flexible or hybrid working arrangements.

Short-term contract work is possible, particularly through recruitment agencies or if you work on a self-employed basis as a consultant.

Related case studies

-

Jonathan Ayodele

Cybersecurity architect

What to expect

- Work is likely to be office-based and you'll typically use a computer for extended periods of time. However, if you work as a consultant then you may need to travel to meet with clients.
- You'll need to have security clearance for certain roles, particularly if you're working for a government agency or private organisation that handles sensitive information. You may also be restricted in terms of what you can say about your work.
- Jobs are available in major cities and large towns throughout the UK. According to Cybershark Recruitment's annual salary survey, growth areas include the North West and South East of England, Scotland and Northern Ireland.
- Self-employment is an option for experienced analysts. You could set up your own cyber security company or work as an independent cyber security consultant. You could also work as a contractor through an agency.
- Although more companies are addressing the gender imbalance, women are still underrepresented in cyber security (particularly at the top level), and in the IT sector as a whole. This is a recognised issue, and steps are being taken to redress the balance. For example, there are organisations which aim to promote greater workforce diversification, such as Cyber Security Challenge UK. Other examples of initiatives aimed

at attracting women into the industry include WISE, WeAreTechWomen, Women in Tech and Women in International Security (WIIS).

- As a consultant working for a company, you'll have to travel within the UK and possibly internationally to visit clients. Independent consultants can be based anywhere and travel to meet clients.

Qualifications

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

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

Alternatively, you could do a degree apprenticeship, where you combine paid work and study towards a recognised qualification. Relevant apprenticeships include:

- Level 6 Cyber security technical professional
- Level 6 Digital and technology solutions - has a cyber security analyst specialism.

It's also possible to enter the profession with a non-technical/unrelated degree. Some graduate schemes, for example, welcome graduates from any degree discipline who have a passion for technology and cyber security. You'll need to have technical skills and an understanding of cyber threats and how they can be prevented, as well as the ability to learn quickly and work as part

of a team. As you gain experience, your degree subject will be less important, and employers will be more interested in what you've done professionally.

Although a postgraduate qualification isn't essential, you could do a Masters degree in a relevant subject, particularly if your degree is in an unrelated subject. Some employers may sponsor you to undertake a relevant Masters course.

Search for postgraduate courses in cyber security.

The National Cyber Security Centre certifies a number of degree apprenticeships, undergraduate, integrated Masters and Masters degrees in cyber security and closely related fields that meet an appropriate educational standard. For a list of courses, see NCSC-certified degrees.

There are also opportunities to move into a cyber security role after gaining experience in a more general IT role.

It's possible to enter the cyber security profession without a degree. There are a range of relevant apprenticeships available at Levels 3 and 4. You can also start in an entry-level IT position and then work your way up to a cyber security role by gaining experience and industry certifications.

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
- analytical and problem-solving skills to identify and assess risks, threats, patterns and trends
- 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

- teamworking skills for collaborating with team members and clients
- time-management and organisational skills to manage a variety of tasks and meet deadlines
- the ability to multitask and prioritise your workload
- excellent attention to detail
- the ability to work under pressure, particularly when dealing with threats and at times of high demand.

Work experience

Employers will expect you to demonstrate a passion for, and an understanding of, the cyber/information security field and you'll usually need relevant pre-entry work experience to get a job. However, there are graduate schemes and internships available (at student and graduate level) in cyber and information security that don't require pre-entry experience.

If it's an option on your course, you could undertake a 12-month industrial placement in a cyber security role. Alternatively, you could contact organisations that employ cyber security analysts and ask to undertake a period of work experience or shadowing. However, there may be restrictions on what you're allowed to do and see.

Making connections with people in the industry and attending relevant cyber and information security events could help you to access opportunities, which may not always be advertised.

If you're studying an IT-related course, you can join BCS, The Chartered Institute for IT as a student member for a small fee to access networking opportunities, mentoring and industry information. Other organisations you can join as a student include the Chartered Institute of Information Security.

The Cyber Security Challenge UK is another source of opportunities. They deliver a series of national competitions designed to test your cyber security skills and host virtual areas designed to support and enhance cyber talents through gamification. The aim is to make cyber security more diverse, inclusive and accessible.

Find out more about the different kinds of work experience and internships that are available.

Cyber security professionals are employed by a variety of organisations across both the public and private sector. You may be working on the security of the organisation you work for or offering security services or consultancy to other companies.

The types of organisations you could work for include:

- professional services
- security consultancies
- information technology companies and network providers
- financial services institutions
- government departments
- energy companies
- transport and logistics companies
- the media
- schools, colleges and universities.

Look for job vacancies at:

- CWJobs
- Cyber Security Jobs
- CyberSecurityJobsite
- ITJobsWatch
- Technojobs

Vacancies are also advertised on professional networking sites such as LinkedIn and on the social media pages of relevant employers.

Specialist recruitment agencies such as Cybershark Recruitment and Barclay Simpson also advertise vacancies.

Where no suitable job is advertised, you can make a speculative application. Make sure you tailor your CV and cover letter to the company you are applying to and seek support from your careers service.

Professional development

Training often takes place on the job, and you may receive mentoring support and advice from more experienced colleagues.

Some employers offer graduate training schemes, which typically last up to two years and involve undertaking a range of placements on rotation. Your employer may fund you to complete an MSc in information/cyber security while you're on the programme.

Cyber security is a fast-moving profession, so you'll need to keep up to date with developments, trends and changes in the sector throughout your career. You can do this by reading the specialist press, reports, blogs and social media, and attending events and conferences. You can access industry information, events and networking opportunities through membership of organisations such as:

- BCS
- Chartered Institute of Information Security
- Information Systems Security Association (ISSA)

The NCSC certifies courses that have been assessed as offering high-quality cyber security training through its NCSC Certified Training scheme. These courses are delivered by a range of training providers at different levels: an 'awareness' level for those new to cyber security and an 'application' level which is more in-depth.

Relevant industry-related certifications are provided by a number of organisations. The UK Cyber Security Council Certification Framework allows you to search for certifications in a range of specialisms, which may be useful to you at different stages of your career. Find a certification.

It's a good idea to look at job adverts for cyber security analyst roles to get a feel for which certifications employers are looking for and to speak to your employer before choosing a certification. Knowledge of General Data Protection Regulation (GDPR) is also useful.

The UK Cyber Security Council has recently been granted Royal Chartered Status to award professional titles to people working in the cyber profession. This means that you can now follow a clear progression route throughout your career from Associate, to Principal and then Chartered professional status. Registration will provide proof of your skills, experience and commitment to continuing professional development and ethical standards. Find out more about professional registration.

Career prospects

Cyber security is a fast-growing field and cyber security skills are in demand, especially for those with the right combination of skills, knowledge and experience. There is likely to be more scope for career progression within larger organisations and financial services institutions.

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.

Achieving relevant certifications is helpful for your career development and progression as many employers specify these as role requirements. There is now also the opportunity to become chartered.

After gaining extensive 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. Setting up your own cyber security company or working as an independent cyber security consultant may also be possible.