Cyber Security Analyst

Cyber security analysts deal with protecting clients' computer systems and information from security risks. They identify problems and develop plans to protect information from threats such as unauthorised access, data theft or file damage and data loss.

The Work

You would deal with a wide range of threats to electronic data including hacking, scammers, viruses, spyware, deliberate information overload, and corruption of data.

You could be:

- looking for potential security threats to a client's computer systems, networks or data, such as illegal data access or changes, or deliberate or unintentional file damage
- developing and putting a security strategy in place to protect data systems against any threats
- investigating and responding to security breaches, such as people trying to get access to information who shouldn't be
- utilising encryption methods and firewalls (protecting a network), monitoring file usage, and deciding who gets access to information on a network
- installing and upgrading security software and testing new products
- monitoring client firewalls, networks and other devices
- testing network systems, and looking for any weaknesses or security holes
- giving technical advice to clients, or training employees in security awareness and procedures
- preparing reports for clients, making recommendations for solutions including hardware and software programmes.

Pay

The figures below are only a guide. Actual salaries may vary, depending on:

- where you work
- the size of the company or organisation you work for
- the demand for the job.

Starting salaries are around £25,000 to £30,000 a year. This would rise to between £33,000 and £60,000 a year experience. Those in a senior position could earn up to £70,000 a year.

Your salary can vary if you work as a consultant or are freelance.

Conditions

- You would be based in an office if you work for a company.
- If you work as a consultant, you would travel to clients' offices or meetings.
- Working hours are 35-40 hours a week, but you might have to work overtime depending on the project

you are working on.

- You might sometimes have to be on call to deal with unexpected problems on evenings or weekends.

Getting In

Although most entrants have a degree (SCQF Levels 9-11) in cyber security or related discipline, it is possible to enter this profession at entry level or apprenticeship and work your way up.

- Abertay, Edinburgh Napier, Glasgow Caledonian, Heriot-Watt, Robert Gordon and the West of Scotland universities all offer relevant degree courses in computer forensics, cyber security or ethical hacking. Entry requirements are usually 4 Highers including Maths or Computing Science.
- Other relevant courses include; computer science, computer engineering, electrical engineering, information technology, or mathematics.
- Entry requirements for degree courses are normally 4-5 Highers including Maths or a science or technological subject, plus National 5 English.
- Relevant postgraduate (SCQF Level 11) courses are available at several Scottish universities. For entry you would normally require a good Honours degree in a relevant subject, or equivalent degree with relevant experience. Check individual institutions' websites for details.
- You might be able to get in through a Graduate Apprenticeship in Cyber Security. This is available at two levels, SCQF Level 10 and 11. For Level 10 you for normally require 4 Highers including Maths and Computing Science. For Level 11 you would require a relevant Honours degree, or the Level 10 Apprenticeship. Check the apprenticeship.scot website for details.
- You could enter through a Modern Apprenticeship in Digital Technology: Cyber Security at SCQF Level 6, or the Technical Apprenticeship at SCQF Level 8. You will learn about the threats to computer networks and systems from criminal cyber-attacks and how they can be prevented.
- You could start at entry level as an IT support technician, developer or network engineer with an NC (SCQF Levels 4-6), HNC (SCQF Level 7) or HND (SCQF Level 8) in Cyber Security. You could work your way up by taking further training and qualifications.
- It helps to get as much experience as you can, or gain experience in an IT related discipline.

Job prospects are good as more organisations rely on the internet and IT services to run their businesses. In particular, organisations normally most at risk from internet threats and attacks are financial organisations, such as banks, local and central government and military organisations.

Some large organisations, such as BT, Network Rail and energy companies, offer apprenticeships and school leaver programmes in cyber security.

What Does It Take

You need to have:

- a keen interest in and aptitude for IT
- good writing and presentation skills to communicate findings
- knowledge of information security threat types
- excellent attention to detail
- a logical systematic and analytical approach

- excellent problem solving skills.

You need to be able to:

- keep up to date with the latest IT developments, standards and legislation
- understand the business needs of your company or client
- work under pressure to deadlines
- understand the laws relating to information and data security.

Training

- You would probably start out as a security analyst and work your way up to security consultant with experience on the job.
- As a Graduate Apprentice you would work and study towards the BEng Hons Cyber Security (SCQF Level 10) or Masters degree in Cyber Security (SCQF Level 11).
- For the Modern or Technical Apprenticeship in Digital Technology: Cyber Security, you would study towards the Diploma in Digital Technology: Cyber Security at SCQF Level 6 or 8.
- You will need to keep up to date with the latest developments in cyber crime, and learning new investigative methods and software. Cyber crime is an ever changing and fast moving area.
- You would learn scripting languages and database development (such as Java, C#, WPF, MySQL, Oracle) as well as operating systems, such as Windows, iOS (Apple Macintosh), Linux, UNIX or DOS, and networking.
- You can study for a range of specialist IT security qualifications such as those offered by ISACA, (ISC)2 or the Chartered Institute of Information Security (CIISEC).

Getting On

- With experience, you can move on to IT analyst or IT security manager jobs.
- You could become self-employed on a freelance basis.
- You could work as a consultant advising different organisations.

More Information

The term cyber security covers the security of the internet, telecommunications networks and computer systems. As more organisations realise the importance of data protection due to their business relying on the internet and IT systems, the prospects for security professionals has never been better.

You should check out **The Cyber Security Challenge** website, a government and industry initiative encouraging involvement in the industry through a variety of interactive games and activities, and providing information on how to start a career in this ever evolving and growing area.

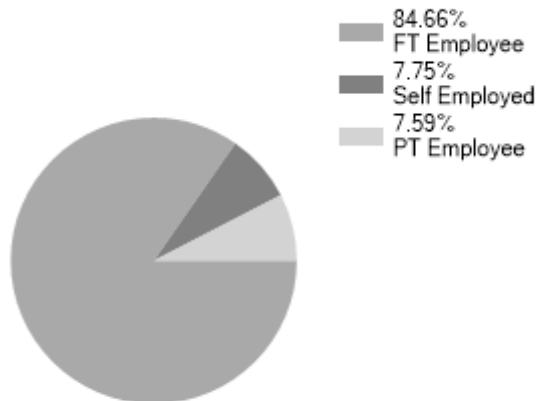For more information please the organisation listed below:

- BCS, The Chartered Institute for IT

Contacts

Statistics

Employment Status UK %

84.66%
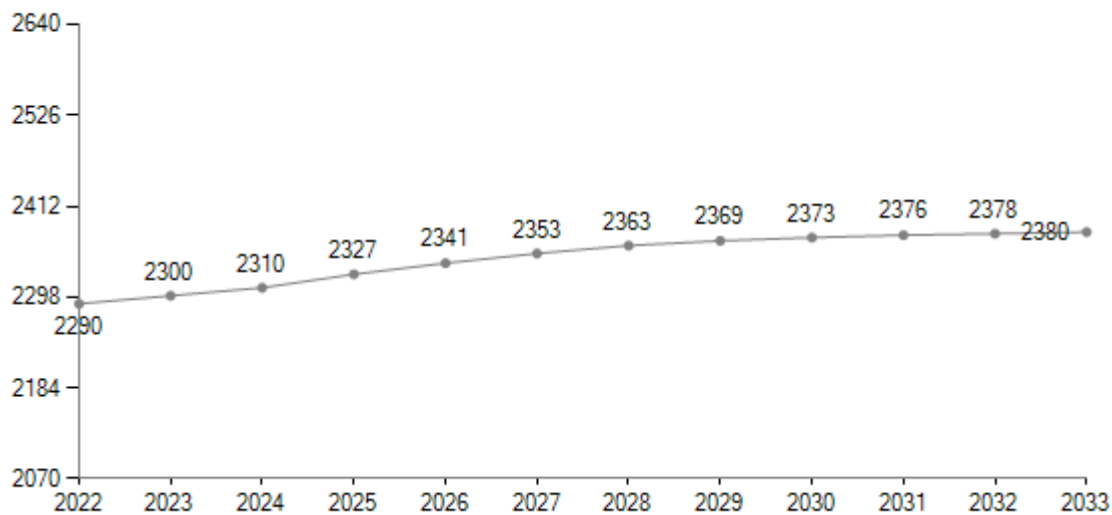FT Employee

7.75%
Self Employed

7.59%
PT Employee

Past Unemployment - Scotland

No Claimant statistics available for Scotland.

LMI data powered by LMI for All

Predicted Employment in Scotland

LMI data powered by Lightcast