Cyber security

What is cyber security?

Cyber security is also known as computer security, forensic technology and covers cryptology and cryptography.

It refers to the security of the internet, wider telecommunications networks and computer systems and its purpose is to defend against web-based or electronic attacks targeted at government, organisations and individuals. These attacks are often very difficult to detect.

The three main areas that graduates may go in to are:

- **Threat management / Risk analyst / Security analyst**

  This may be working in an organisation's IT department to keep cyber attacks at bay, or working as a consulting for a client, assessing their security and advising on security strategies. You will need to have strong problem solving skills and be able to react quickly to incidents and crisis. You will need to communicate in non-technical terms to managers who may have to make difficult quick decisions.

  As cloud computing gains ground, there will be increased demand for these professionals as many companies are concerned about their security and data confidentiality.

- **Ethical hacking, penetration testing**

  These roles involve simulating cyber attacks on computer systems for the purposed of discovering and eliminating security vulnerabilities. Also known as penetration testers, ethical hackers need analytical and problem-solving skills, as well as excellent judgment and self-motivation.

  Qualifications and experience: An enquiring mind, persistence and integrity are as vital as any formal qualification. A track record of solving security problems is also a pre-requisite. More industry qualifications are emerging in this fast-growing profession. You can acquire the certified ethical hacker (CEH) badge after a week's course. However the emerging gold plate of ethical hacking is the Council of Registered Ethical Security Testers (CREST), which is allied to the government-approved CHECK scheme.

  There's a shortage of cyber security skills in the UK, according to the national sector council, e-skills. There will be opportunities in many areas, especially in financial services, energy and government sectors.

- **Engineering, Architecture and Design**

  These roles may be dealing with hardware or software, design and development or secure applications. Their purpose is to get the design of a system right, to prevent attackers from getting in. As the situation is constantly changing you have to move quickly to be ahead of the game.

  Sales and marketing is often an essential part of the business.

Salary and progression

Average starting graduate salaries are between £25-32,000, with potential for much higher earnings for experienced analysts.

Most large organizations employ cyber security experts, either in-house or through a consultancy. There are some graduate schemes, such as:

- PwC - Forensic technology
- Deloitte - Forensic technology
- KPMG – Technology Risk Consulting
- Thales e-Security – Graduate Software Engineer

Professional bodies

There are currently a number of professional bodies for this industry:

The Institute of Information Security Professionals
The principal objective of the IISP is to advance the professionalism of information security practitioners and thereby the professionalism of the industry as a whole. The Institute is an independent not-for-profit body governed by its members, ensuring standards of professionalism - for training, qualifications, operating practices and individuals.

Cyber Security Challenge UK Ltd
Cyber Security Challenge is a not for profit company that aims to bring more talented people into the Cyber Security Profession. It is sponsored by professionals from the public and private sector who recognize the need to bring young talent to the cyber security industry.

Where could you work?

- **Police forces**
- **Government agencies (Customs & Excise, DTI, Serious Fraud Office)**
- **Government intelligence services, including GCHQ**
- **Specialist forensic computing firms**
- **Software developers producing encryption software**
- **IT security and corporate investigation companies**
- **Large chartered accountancy firms**
- **Banks and credit card companies**

Labour market

The rising demand for cyber security expertise in the UK presents an opportunity for graduates to build a career in an emerging field: there are opportunities in the financial services, energy and government sectors especially. There are a range of roles opening up in both technical and non-technical positions, from penetration testers to policy makers and managers.

Recently the government announced its new National Cyber Security Strategy[1]. The DEVELOP strand of the strategy emphasises the importance of "strengthening cyber security skills" and "stimulating growth in the cyber security sector". The message from government and industry is clear: there are opportunities for people with required skills in cyber security. However, the lack of technical expertise to fill these vacancies is particularly marked; consequently a number of government initiatives have been set up to address the shortage.

[1] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

When launching its original Cyber Security Strategy, the UK Government allocated £650m of funding over four years to establish a National Cyber Security Programme (NCSP) to strengthen the UK's cyber capability. Amongst the key activities it included was setting up the new Cyber Crime Unit and the creation of the new Joint Cyber Unit hosted by GCHQ.

A survey of UK cyber security employers by the SANS Institute[2] found that they are frustrated by the time it takes to recruit new cyber security talent with the practical knowledge and hands-on skills needed to make an immediate impact on the job. Vacancy data from IT Jobs Watch, together with supporting information from the ONS Quarterly Labour Force Survey[3] estimate there are approximately 58,000 cyber security specialists working in the UK: in 2016 just under 7,000 positions for cyber security specialists were advertised, an increase of 18% on the previous year and 103% on the level five years earlier.

Routes into cyber security

An MSc in Computer Security, Information Security, Computer Forensics, at one of the UK universities awarded Academic Centre of Excellence status in Cyber Security Research[4]:

Many other institutions offer an MSc in Cyber Security or related subject, including the Open University.

There are some graduate schemes and graduate level jobs for graduates of any discipline. Some jobs and courses require a degree in computer science or a related subject. The most important attributes are a passion for technology and an enquiring mind.

Sources of vacancies

- Careers Centre vacancy database – https://mycareer.leeds.ac.uk/home.html
- Serious Fraud Office - https://www.sfo.gov.uk/about-us/careers/
- Cyber Security Challenge https://cybersecuritychallenge.org.uk/careers/jobs-internships
- Lawson Chase - www.lawsonchase.com/
- SANS CyberTalent Immersion Academy Employment - https://www.sans.org/cybertalent/immersion-academy/employment
- Secret Intelligence Service – SIS (MI6) - https://www.sis.gov.uk/explore-careers.html
- National Cyber Security Centre https://www.ncsc.gov.uk/articles/careers-national-cyber-security-centre
- International Association for Cryptologic Research - http://www.iacr.org/jobs/
- Prospects - http://www.prospects.ac.uk/
- Milkround - http://www.milkround.com/search/
- Inside Careers - http://www.insidecareers.co.uk/
- TargetJobs - http://targetjobs.co.uk/

[2] http://www.sans.org

[3] https://www.ons.gov.uk/employmentandlabourmarket

[4] https://www.epsrc.ac.uk/research/centres/acecybersecurity/

Would it suit you?

The majority of these opportunities are currently for people with technical skills. Typically, people working in this area have an academic background in computer science. However, if you don't have this academic background but have a passion for technology, don't be put off! Government and industry are keen to encourage those with relevant skills.

It is also about attitude and mindset. Cyber security requires you to constantly question the world around you. Practitioners are often natural cynics, enjoy probing complex problems and expect nothing to be as it first appears. Like the attacking communities they defend against, they are creative and adept at thinking outside the box.

To succeed in the industry you must have an urge to understand things completely - to take them apart, find out how they work and identify their weaknesses. Whether it's a mobile handset, a complex application or an organisation's knowledge management system, we must understand how it works and how it could be attacked.

There is also a strong human element too; you will have to communicate with a broad audience from management to junior staff, both the technically-aware and the technology-averse alike.

Cyber Security Challenge UK is a government and industry initiative open to people from any background. The Challenge involves a series of tasks and competitions designed to identify people with cyber security skills with prizes including paid internships and bursaries for relevant university courses. Even if you do not want to participate in the Cyber Security Challenge their website provides a useful resource for understanding what a career in cyber security could look like and how to get involved.

Qualifications and Skills required

The IISP Skills Framework[5] describes the range of competencies expected of Information Security and Information Assurance Professionals in the effective performance of their roles. It was developed through collaboration between both private and public sector organisations and world-renowned academics and security leaders.

- Teamwork and Leadership
- Delivering – project and results
- Managing Customer Relationships
- Corporate Behaviour
- Change and Innovation
- Analysis and Decision Making
- Communication and Knowledge Sharing

It is more common for advertisements for cyber security jobs to require certification than for other digital roles, the most common ones currently are CISSP and ISO/IEC 27001.

[5] https://www.iisp.org/imis15/iisp/About_Us/Our_Skills_Framework/iispv2/Accreditation/Our_Skills_Framework.aspx?hkey=e77a6f03-9498-423e-aa7b-585381290ec4

Work experience

Work experience is important for any role. Although the number of graduate entry level positions in IT has doubled over the last 10 years, over a third of recruiters surveyed reiterated their warning that graduates who have no previous work experience have little or no chance of receiving a job offer [6].

There are work placements and experience opportunities in this sector, but any work experience that allows you to develop and demonstrate the skills listed above will be helpful.

Sources:

- Careerweb http://careerweb.leeds.ac.uk/
- Prospects http://www.prospects.ac.uk/
- TargetJobs http://targetjobs.co.uk/
- Inside Careers: Technology in Finance and Consultancy http://www.insidecareers.co.uk/professions/it/advice/about/overview-ofthe-it-industry/
- Inside Careers: Hot Topics – Cyber Security http://www.insidecareers.co.uk/career-advice/cyber-security/
- Tech Partnership Factsheet: Cyber Security Specialists in the UK https://www.thetechpartnership.com/globalassets/pdfs/research-2017/factsheet_cybersecurityspecialists_feb17.pdf
- Centre for the Protection of National Infrastructure http://www.cpni.gov.uk/
- National Cyber Security Centre https://www.ncsc.gov.uk/
- Gov Info Security www.govinfosecurity.com/
- Information Assurance Advisory Council www.iaac.org.uk/
- Internet Crime Forum www.internetcrimeforum.org.uk
- National Crime Agency http://www.nationalcrimeagency.gov.uk/
- National Cyber Crime Unit http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit
- University of Kent: Biometrics, Forensic Computing, Computer Security and Cryptography Careers https://www.kent.ac.uk/careers/workin/forensiccomputing.htm
- Guardian: Behind the Job Title: Cyber Security Consultant https://www.theguardian.com/careers/working-in-cyber-security
- Vega Consulting http://www.vega.co.uk/in focus/uk cyber security strategy 09.aspx
- University of Edinburgh Careers Service: Careers in Cryptology, Codes, Code-Breaking and Encryption http://www.ed.ac.uk/files/imports/fileManager/Careers_in_Cryptology.pdf
- Reaction Information Security http://www.reactionpenetrationtesting.co.uk/penetrationtesting.html
- ISACA Journal: the Underestimated Social Engineering Threat in IT Security Governance and Management http://www.isaca.org/Journal/archives/2015/Volume-3/Pages/the-underestimated-social-engineering-threat.aspx
- IISP - Institute of Information Security Professionals http://www.iisp.org/
- Government documents: National Security Strategy 2016-2021 - https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
- EC-Council: Certified Ethical Hacking Certification https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
- IT Governance: CISSP (Certified Information Systems Security Professional) https://www.itgovernance.co.uk/cissp
- CREST http://www.crest-approved.org/
- ISO/IEC 27001 Information Security Management http://www.iso.org/iso/iso27001
- EPSRC: Academic Centres of Excellence in Cyber Security Research https://www.epsrc.ac.uk/research/centres/acecybersecurity/

[6] High Fliers survey 2017

- High Fliers Survey 2017 http://www.highfliers.co.uk/download/2017/graduate_market/GMReport17.pdf
- Cyber Security Challenge: Developing a cyber talented and security aware workforce https://cybersecuritychallenge.org.uk/inside-cyber/developing-cyber-talented-security-aware-workforce
- IT Jobs Watch http://www.itjobswatch.co.uk/
- Office of National Statistics Quarterly Labour Force Survey https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/qmis/labourforcesurveylfsqmi
- National Guidance Research Forum http://www2.warwick.ac.uk/fac/soc/ier/ngrf /
- Association of Graduate Recruiters https://www.agr.org.uk/Home

Georgina Larkin - May 2013
revised by Janet Hindle – February 2017