Report ID-0333

Helpdesk Report:

Cyber Security and Networks Manager

by

Incomes Data Research

August 2022

This report has been produced by Incomes Data Research Limited as part of the ECC Labour Market and Pay Data Service.

Any queries relating to this report should be directed to:
t: +44 (0) 1702 669549
e: marketdata@incomesdataresearch.co.uk

Incomes Data Research Limited. Registered in England & Wales. Company No. 09327550.
Registered address: 71-75 Shelton Street, London WC2H 9JQ

Correspondence address: Incomes Data Research, The Studio, The Old Gasworks, 43 Progress Road, Leigh on Sea, Essex SS9 5PR

Contents

1. Introduction

This report has been prepared by Incomes Data Research (IDR) and, as requested, it provides market salary data for the following role(s):

- Cyber Security and Networks Manager

2. Market salary data

This section presents the market salary data. We aim to provide a minimum of three sources of information for each job to enable 'triangulation' of the results, and thereby provide the widest possible assessment of the market for this role.

2.1. Market data

The tables in the following sections provide the aggregate market salary for a full-time • Cyber Security and Networks Manager.

2.1.1. NHS data

In this section we provide information on the salary range for the pay band likely to cover comparator jobs in the NHS. The NHS, with 1.2m staff is the largest employer in the UK and as such plays a key role in influencing the market for many non-medical roles, particularly in education, given the links between parts of higher education and the NHS.

Cyber/Security managers in the NHS are typically employed on Band 8a or Band 8b depending on the size of the trust. The current salary range is between £48,526 and £54,619 (Band 8a) and between £56,164 and £65,262 (Band 8b) a year outside of London and high-cost areas in the South East/South.

Roles based in high-cost areas qualify for the following supplements:

- Inner London – 20% of basic salary, subject to a minimum payment of £4,888 and a maximum payment of £7,377;

- Outer London – 15% of basic salary, subject to a minimum payment of £4,108 and a maximum payment of £5,177;
- Fringe – 5% of basic salary, subject to a minimum payment of £1,136 and a maximum payment of £1,915.

2.1.2. IDR data

The following tables contain data from IDR Pay Benchmarker, our online database of salary information. This data has been collected by IDR directly from employers through surveys and bespoke data collection for the IDR Pay Benchmarker service.[1]

Cyber Security Manager, public sector, job level 8

Job level	Company count	Lower quartile	Median	Upper quartile	Average
Level 8	12	£52,750	£54,669	£58,303	£54,857

Source: IDR Pay Benchmarker.

2.1.3. Recruitment data

The data in this section is based on analysis of recruitment salaries for a similar role(s). It is a guide to starting pay for these roles, and in some cases also provides a guide to the maximum that might be achieved.

IT & Cyber Security

Job role	Range £pa	Average £pa
Cyber Security Manager, North of England	£35,800 to £57,800	£46,800
Network Security Manager, North of England	£38,100 to £56,700	£47,400

Source: Reed Salary Guide 2022, Technology.

[1] Refers to the IDR Job Level. These typically cover the following types of roles: 1 and 2, admin, support and manual roles; 3 and 4, secretarial and craft roles; 5 and 6, vocational and supervisory; 7 and 8, professional and managerial; 9, senior management; 10a and 10b, directors; 11, senior directors/chief executives.

3. Job advertisements

This section details current comparable vacancies from our database of advertised positions.

3.1. Data and summary

Cyber Security and Networks Manager - job advertisements

Reference ID	Organisation	Job title	Min	Max	Location
ID630	St George's, University of London	Cyber Security Operations Manager	£43,414*	£51,805	London
ID632	Department for Work & Pensions	Senior Cyber Security Risk Manager**	£50,155	£50,155	North West/North East/Yorkshire

*Plus London allowance of £3,291pa. ** Note that two jobs are included in the advert

3.2. Job advertisements

The following pages present the job advertisements for the above vacancies.

Cyber Security Operations Manager

Information Services

Salary: £43,414 to £51,805 plus London Allowance of £3,291 per annum
Permanent, full time position
Opening Date: Wednesday 17 August 2022
Closing Date: Sunday 18 September 2022
Interview Date: To be confirmed
Reference: 906-22

We are looking to appoint an exceptional cyber security professional to join IT Services. The post holder will play a pivotal role in leading the University in its cyber defence efforts, protecting its staff and data. We would like to hear from highly competent candidates who have achievements in cyber security and who is keen to progress their skills in a University setting.

Key attributes of the successful applicant (*no more than 50 words*) include:

- Strong, up-to-date cyber security skillset

- Ability to work under pressure
- Passion for delivering a great service and good customer service
- High level of prioritisation and organisation to manage a high volume of work and priorities effectively
- Strong organisational, time-management and communication skills
- Enthusiasm and personal initiative to solve problems, a self-starter with ability to work unsupervised

For further information about this position and to apply, visit http://jobs.sgul.ac.uk.

We welcome and encourage applications from underrepresented groups, especially from people with disabilities and/or people from ethnic minority backgrounds.

Flexible working, including part-time or reduced hours of work, opportunities to work from home for many posts, compressed hours and local flexibility in agreeing start and finish times of work are among the extra benefits offered by St George's, University of London.

Please quote reference: 906-22

Closing date: Sunday 18 September 2022

Interview date: **TBC**

Email details to a friend Apply Online

Further details:

- Job Description

St George's is an Equal Opportunities Employer

No agencies please

St George's, University of London: the UK's only university dedicated to medical and health sciences education, training and research

St George's, University of London

Information Services

Cyber Security Operations Manager

Ref: 906-22

JOB DESCRIPTION

Post Title	Cyber Security Operations Manager
Grade	SGUL 7
Contract type	Permanent
Responsible to	Head of Infrastructure
Accountable to	Assistant Director (IT Services)
Responsible for	Institutional Cyber Security Strategy and Assurance inc. Cyber Security Certifications Cyber Security Analyst
Liaises with	IT Services, Information Governance, administrative departments, research institutes, Library, SGUL academic staff, external suppliers, Centre for Technology in Education and Learning Technology Services.

Overall purpose of job

1. The main purpose of this role is to provide strategic leadership and guidance on cyber security strategy and cyber operational matters. It will lead investigations into any IT related breaches and cyber-attacks. The role will also plan financially to support the cyber strategy.

2. Main Duties and Responsibilities

- Provide advice on IT security related issues to the university in a timely manner
- Development and delivery of cyber security projects for the business
- Promoting responsible behaviour and the cybersecurity culture to ensure staff, students and infrastructure are protected against all potential cyber threats.
- Defining and building an effective cyber threat-intelligence capability (people, process and systems)
- Implement and manage effective vulnerability assessments

- Oversight of cyber security threat incident response and investigations
- Manage and obtain the relevant cyber security certifications

Main Duties and Responsibilities

- Contribute to business continuity planning and disaster recovery plans for IT Service's datacentres across the University
- Working with the Information Governance Manager you will be responsible for planning and development of an appropriate Information Security operational plan. Leading the development of information security architecture, services and systems within the University environment.
- Team Management of the cyber security analysts, planning and implementing effective training, CPD programmes and personal development plans.
- Responsible for the selection, implementation and operation of cyber security services and solutions
- Stay abreast of information security issues and regulatory changes affecting higher education, participate in national policy and practice discussions, and communicate to the University on a regular basis about those topics; engage in professional development to maintain continual growth in professional skills and knowledge essential to the position.
- Utilising analytical tools to determine emerging threats, vulnerabilities and implement measures, such as Intrusion Detection and Prevention and encryption to find the best way (with support as necessary) to secure the IT infrastructure
- Ensure regular reviews of policy documents are conducted. Advising the relevant committees of proposed changes.
- Work with other ICT colleagues to ensure that systems are patched and adequately secured and protected, and that any changes are performed in a controlled and documented fashion
- Maintain a strategy and plan for information security work which addresses the evolving business risk and information control requirements.
- Carry out regular security audits both internal and with the assistance of external security specialists
- Regular inspections of systems and functions to ensure compliance with university policy and to ensure that any gaps are filled
- Engage directly with university projects to review new projects and initiatives, ensuring security requirements are captured and managed through to implementation
- Responsible for the process of gathering, analysing and assessing the current and future threat landscape, providing a realistic view of risks, threats and priorities in the enterprise environment
- Lead investigations, analysis and review following breaches of security controls and manages security incidents
- Communicate well, both orally and in writing, and respond to wide-ranging and detailed questioning relating both to own areas of specialisation and, at a more general level, to the wider field of IT
- Promote the service within the University and create strong personal relationships with the full range of stakeholders.
- Liaise with HE sector, external organisations and key suppliers to share ideas, compare approaches and develop best practice.
- Co-ordinate cyber security awareness training for colleagues

It is expected that staff working at St George's, University of London will be involved in our mentoring and tutoring activities, as appropriate, as well as supporting admissions, student recruitment and access and widening participation activities (MMI interviews, Open Days, school visits, clearing etc) where applicable. All academic staff are expected to act as a personal tutor.

You are also expected to undertake other activities appropriate to your grade as directed by your manager. This job description reflects the present requirements of the post. As duties and responsibilities change, the job description will be reviewed and amended in consultation with the post holder from time to time. St George's, University of London aims to provide opportunities for all its employees to develop the skills required to be successful in their role and to further develop their careers.

St George's, University of London, is committed to the San Francisco Declaration on Research Assessment (DORA) principles.

3. Special Factors

- IT Services' normal hours of operation are currently 9am - 5pm weekdays, with a weekly "At-Risk" period; 7am - 9am on Tuesday mornings. It is expected small service changes affecting systems would be performed in this window. The role holder would be expected to be in attendance where their services are required.
- Additionally, there are times when extended hours of downtime are required which is scheduled at weekends, it is expected the role holder will make themselves available for such out of hours work when given appropriate notice.
- Be available in times of emergency and be an integral part of IT Services' business continuity and disaster recovery team.

For information, St George's, University of London and Royal Holloway, University of London have agreed to progress discussions about a potential merger. Further information is available here.

More information about St George's, University of London can be found at www.sgul.ac.uk.

St George's, University of London currently offers a range of employee benefits:

Salary:	**£46,705** pa, including London Allowance (pro-rated for part-time staff). The salary range for **SGUL 7** is **£46,705** – **£55,096** including London Allowance, but appointment is usually made at the minimum point.
Hours:	35 hours per week which can be done flexibly in various ways or part time/job share can also be considered. Staff are expected to work the hours necessary to meet the requirements of the role and this will be dependent on the service area.
Annual leave:	32 days per annum. Plus eight UK public holidays and three days when St George's, University of London is closed (usually between Christmas and New Year). Part time staff receive a pro rata entitlement.
Pension:	Membership of competitive pension schemes with generous employer contribution and a range of extra benefits. Superannuation Arrangements of the University of London (SAUL) Universities Superannuation Scheme (USS) National Health Services Pension Scheme (NHSPS) (existing members only)
Flexible working	Flexible working, including part-time or reduced hours of work, opportunities to work from home for many posts, compressed hours and local flexibility in agreeing start and finish times of work.
Travel	St George's, University of London offers an interest free season ticket loan and participates in the Cycle to Work Scheme.
Gift Aid	If you would like to make a tax-free donation to a charity of your choice, this can be arranged through our Payroll.
Sports and Leisure Facilities	Rob Lowe Sports Centre, situated on the St George's Healthcare NHS Trust site offers exercise facilities that can be utilised by St George's, University of London staff. Within walking distance from the University is Tooting Leisure Centre. Facilities include a swimming pool, gym and various exercise classes. The Centre offers SGUL staff an all-inclusive corporate membership. For more information please contact Tooting Leisure Centre.
Shops and facilities	There are a number of shops and facilities situated on site including ATMs, student bar and shop, Pret a Manger, M&S Simply Food store, library and multi-faith room.

disability confident EMPLOYER

Athena SWAN Silver Award

Stonewall DIVERSITY CHAMPION

Informal enquiries

Informal enquiries may be made via email to: Hrhelp@sgul.ac.uk

Making an application

All applicants are encouraged to apply on line at http://jobs.sgul.ac.uk as our system is user friendly and the online application form is simple to complete. Please note that s only will not be accepted.

For any accessibility issues please contact hrhelp@sgul.ac.uk

Closing date: **Sunday 18 September 2022**

Interview date will be TBC. As shortlisted candidates will be notified by email, it is imperative that you provide an email address that is accessed frequently.

Please quote reference **906-22**

We are delighted that you are interested in working at St George's, University of London. You will be notified of the outcome of your application by email. We aim to respond to all candidates within 5 weeks of the closing date of the vacancy.

Lead & Senior Cyber Security Risk Manager

Department for Work and Pensions

Apply before 11:55 pm on Thursday 1st September 2022

Reference number

225366

Salary

£50,155 - £81,468

Grade

Grade 7
Grade 6

Contract type

Permanent

Business area

DWP - Digital

Type of role

Digital
Information Technology

Working pattern

Flexible working, Full-time, Job share, Part-time

Number of posts

6

Contents

Location

This role will be based in Blackpool, Leeds, Manchester, Newcastle or Sheffield. Please find further information on the Corporate hub locations here.

About the job

Summary

Are you a Cyber Security Risk Manager that has worked in a large scale organisation?

If yes, we want you to join us at DWP Digital.

These are critical roles co-ordinating and delivering the Digital Security Risk management programme of work, with risk driving security, enabling a clear, practical, and realistic view of Cyber Security Risk information. The role forms a vital First Line capability within the HMG three-line defence model.

As a Lead Cyber Security Risk Manager you will report directly to the Digital Security Risk Management Team Lead, you will Lead within the Digital Group to help deliver 1st line risk identification, assessment, remediation, and treatment of risks. You will lead the work to implement controls and make recommendations to address security vulnerabilities and control weaknesses in products, projects, and programmes, working with product owners and Subject Matter Experts to enable them to make well informed risk-based decisions whilst leading and influencing the management of tactical and strategic risks.

As a Senior Cyber Security Risk Manager you will work within the Digital Group to help deliver 1st line risk identification, assessment, remediation, and treatment of risks. You will identify controls, make recommendations to address security vulnerabilities and control weaknesses in products, projects, and programmes, working with product owners and Subject Matter Experts to enable them to make well informed risk-based decisions whilst leading and influencing management of tactical and strategic risks.

Job description

Lead Cyber Security Risk Manager

• Provide leadership to ensure effective security Risk expertise, advice and support is delivered to include business managers, Senior Risk Owners, and the Executive Team within DWP.

• Providing Security input at board level and working in liaison across the Department and with wider HMG, at both strategic and practical levels, to ensure proportionate, risk-informed decisions about current and future security investments can be taken to protect the Department’s assets and improved the Department’s Security risk position.

• Provide leadership and direction on the implementation of the Digital Governance Risk and Compliance methodology and day to day utilisation of the risk management toolsets at all levels from the design, delivery, and operations support stages. Ensuring the timely recording and updating of risks throughout the lifecycle.

• Provide leadership and direction for the research/evaluation of business processes aligned to known/emerging Security risks and controls.

• Providing Security input at board level and working in liaison across the Department and with wider HMG, at both strategic and practical levels, to ensure proportionate, risk-informed decisions about current and future security investments can be taken to protect the Department's assets and improve the Department's Security risk position.

Senior Cyber Security Risk Manager

• Manage and support Digital's Cybersecurity risk management lifecycle by working to help deliver 1st line risk identification, assessment, remediation, and treatment of risks.

• Drive a culture of effective and accurate security risk management and facilitate the governance of Digital Security Enterprise Risk Management within the four stages of the Security/Fraud Risk management lifecycle.

• Provide thought-leadership to ensure effective security Risk expertise, advice and support is delivered to business managers, Senior Risk Owners, and the Executive Team within DWP.

• Identify controls and make recommendations to address security vulnerabilities and control weaknesses in products, projects, and programmes, working with product owners and Subject Matter Experts to enable them to make well informed risk-based decisions whilst leading and influencing the management of tactical and strategic risks.

• Identify, capture, or contextualise risks and mitigating controls, enabling risk owners and managers to take responsibility for the management and maintenance of their security.

• Work closely with Security & Data Protection and other internal and external stakeholders, to ensure Cyber Security threats, vulnerabilities, and opportunities with the potential to impact or improve resilience of Digital IT Infrastructure are identified, and / or reported appropriately. Take responsibility for delivering timely and quality results with focus and drive.

• Use evidence and knowledge to support accurate, expert decisions and advice. Carefully consider alternative options, implications, and risks of decisions. Support strategic development of the service vision with programmes, enabling the prioritisation and delivery of solutions with appropriate security controls to mitigate Cyber Security Risks through a structured risk management process.

Check out these blogs about how you can help shape the future of Government Cyber Security.

Responsibilities

Technology Services provide the foundations upon which digital services for DWP are developed and operate. Our purpose is to deliver secure, effective and cost-efficient digital infrastructure services and to run live IT operations that support DWP business objectives. We do this by putting users and quality of service at the heart of what we do.

Our team is made up of 1,500 colleagues working collaboratively across 10 portfolio-led teams in a fast-

moving environment. Our teams deliver an end-to-end suite of digital products and services that support DWP colleagues and citizens in an ever-evolving technology landscape. Our work is focused around the following 6 themes:

1. Delivering a digital workplace that improves the way we work. We provide the products and services to make our users' jobs easier, encourage greater collaboration and support flexibility in working patterns, locations and on devices of their choice – helping to drive forward DWP's digital transformation.

2. Delivering high-quality and resilient IT services and support. We are embedding a Full Stack Service Model to integrate our IT operations and ensure our services meet existing and future network demand.

3. Building a world-class performance-focused user experience control centre. We have created an end-to-end, data-driven performance environment to measure our systems and ensure we keep the department functioning.

4. Exploiting and enhancing hybrid cloud services. We provide hybrid cloud services that balance on-premise and public cloud to offer true platform independence and optimum price performance.

5. Protecting and securing our services. We ensure our IT systems remain secure and available, resilient to natural and human-caused disaster – ensuring citizens always have access to our key services.

6. Developing our people, capability and skills. We have created a sustainable service by developing our people, bringing key skills in-house to DWP, giving our teams professional pathways to develop and opportunities to progress within Technology Services.

As we continue our journey to service excellence we have identified a number of opportunities to join our Technology Services team.

Technical skills

We'll assess you against these technical skills during the selection process:

Information Risk Assessment and Management

Applied security capability

Protective Security

Threat Understanding

Benefits

• An employer pension contribution of up to 27% For further information please click here.
• Annual leave rising up to 30 days, (based on your working pattern).
• Family friendly flexible working arrangements, such as hybrid working, job sharing, term-time working, flexi-time and compressed hours.
• Learning and development tailored to your role this could include industry recognised qualifications, coaching and mentoring.
• An inclusive and diverse environment with opportunities to join staff networks including: Women's Network, National Race Network, National Disability Network (THRIVE) and many more.

This job role may be suitable for hybrid working, which is where an employee works part of the week in their DWP office and part of the week from home. This is a voluntary, non-contractual arrangement and your office will be your contractual place of work. The number of days that anyone will be able to work at

home will be determined primarily by business need but personal circumstances and other relevant circumstances will also be taken into account. If you are successful, any opportunities for hybrid working, including whether a hybrid working arrangement is suitable for you, will be discussed with you prior to you taking up your post.

Salary Information

Salary for this role at Grade 6 is from £66,860 (Band min) to £74,392 (Band max).

Where the maximum salary of £74,392 is offered, a Digital Allowance of up to £7,076 per annum is available for exceptional candidates, based on our assessment of your skills and experience.

Salary for this role at Grade 7 is from £50,155 (Band min) to £60,781 (Band max).

Where the maximum salary of £60,781 is offered, a Digital Allowance of up to £5,411 per annum is available for exceptional candidates, based on our assessment of your skills and experience.

Our offer to successful candidates will be based on an assessment of your skills and experience as demonstrated at interview.

Existing Civil Servants who secure a new role on lateral transfer should maintain their current salary.

Existing Civil Servants who gain promotion may move to the bottom of the next grade pay scale or 10% increase in salary whichever would be the greater.

Things you need to know

Security

Successful candidates must pass a disclosure and barring security check.

Successful candidates must meet the security requirements before they can be appointed. The level of security needed is security check.

See our vetting charter.

People working with government assets must complete basic personnel security standard checks.

Selection process details

This vacancy is using Success Profiles, and will assess your Experience and Technical skills.

Stage 1: Application

Applications must include:

1. A completed Personal Details application form.

2. A curriculum vitae including education, professional qualifications and full employment history, giving details of key achievements.

When giving details in your CV you should highlight your experience in line with essential criteria below:

• Leads complex risk assessments, interfacing routinely with senior management.

• Develops complex and innovative information risk management plans under supervision. Develops complex and innovative information risk management plans either as an individual or leading a team.

• Experience of leading corporate threat intelligence processes.

• Experience of leading development of corporate Information Security strategies.

The following criteria is desirable:

• Certified in Risk and Information Systems Controls (CRISC), or equivalent risk management qualifications, and or proven knowledge of risk management frameworks – identification, assessment, risk response and mitigation, control monitoring and reporting.

When giving details of your CV, you should therefore include details of the work and projects that you have been involved in, and your role therein.

For Hints and Tips on completing your application visit our blog Getting Hired at DWP Digital .

Applications will be sifted at regular intervals and candidates will be interviewed on an ongoing basis. Please apply as soon as you can, do not wait until the end of the campaign.

Important information

• Please attach your CV as a separate additional document in either PDF or word format.
• Personal details that could be used to identify you including your name, contact details and address must be removed for your application to be considered.
• Please do not include any personal details in your document title.
• **If your CV contains any personal details your application will be withdrawn.**

Stage 2: Interview

If you're successful at sift stage you will be invited to a video interview via Microsoft Teams. There, you will be assessed against the following Technical Skills:

• Information Risk Assessment and Management -Enables the organisation to deliver balanced and cost-effective risk management decisions on situations with complex scope or significant risk. Ensures that risk is embedded into corporate governance processes.

• Applied security capability - Provides security advice that extends beyond particular technologies of which the candidate is familiar and draws upon and directs appropriate expertise to solve the bigger security problem. Ensures the overall technical coherence and quality of advice.

• Protective Security - Leads innovation in protective security, taking into account other specialisms/enablers and business drivers.

• Threat Understanding - Combines external threat information, organisational context and situational awareness to provide a holistic threat understanding capability, including the use of threat models.

You will be asked to do a short (5 minutes) presentation on a specific topic. Further details will be provided to candidates invited to interview.