## About us...

Lincolnshire Co-op is a long-standing, community-focused organisation proud to serve the people of Lincolnshire and surrounding counties. Our Support Centre, based in Lincoln, is the operational heart of our business. It's home to a range of specialist teams who work behind the scenes to support our front-line colleagues and ensure we deliver exceptional service across all our trading areas.

## Essential Information – *what you need to know*

| | |
|---|---|
| **Job purpose:** | - Supporting the Senior Cyber Security Manager in implementing and managing the Society's cyber security strategy, governance, and operational controls.<br>- Leading cyber operations activity, including threat monitoring, incident response and vulnerability management, to ensure the protection of the Society's systems and data.<br>- Driving a culture of continuous improvement, awareness and pro-active defence across the organisation through collaboration, training, and innovation. |
| **You'll report to:** | - Senior Cyber Security Manager |
| **Your hours:** | - 37.5 hours per week (FTE) |
| **Your relationships:** | - Senior Cyber Security Manager: supporting the delivery of cyber security initiatives, reporting on incidents, risk posture, and ongoing improvements.<br>- IT Infrastructure Team: collaborating to identify vulnerabilities and maintain secure systems.<br>- Head of IT and Digital: providing updates on key risks and operational performance as required.<br>- External suppliers and partners: supporting third-party assessments, SOC services, and threat intelligence sharing. |

| | |
|---|---|
| **What you'll bring to us:** | - A relevant degree in cyber security, computer science, or equivalent experience in a cyber security role.<br>- Proven experience working in SOC operations, incident response, or vulnerability management within a complex IT environment.<br>- Strong technical knowledge of network and infrastructure security, IAM, and data protection controls.<br>- Familiarity with cyber security frameworks and standards such as ISO/IEC 27001, NIST, or CIS.<br>- Excellent analytical and problem-solving skills, with attention to detail and accuracy.<br>- Strong interpersonal and communication skills, with the ability to translate technical issues into clear business language.<br>- Collaborative mindset, with experience working across IT, Risk, and Compliance functions.<br>- Pro-active approach to learning and staying current with emerging threats, tools, and best practices.<br>- Experience in managing or supporting third-party security service providers.<br>- Good understanding of regulatory requirements, including GDPR and data privacy standards.<br>- Confidence in delivering training and awareness to technical and non-technical audiences.<br>- Strong organisational and time management skills, capable of managing multiple priorities simultaneously.<br>- A full UK driving licence and access to a vehicle for business use. |

# Our Purpose

*Bringing together energy, ideas and resources to make life better in our communities*

## Together we are

**Providing and supporting** valued services

**Helping to grow the** local economy

**Caring for our** health and wellbeing

**Looking after our** local environment

## Your Purpose – *I will contribute to my team and the Society's ongoing success in this role by...*

**Your duties and responsibilities:**

- Supporting the Senior Cyber Security Manager in the delivery of the Society's cyber security roadmap, aligning activity with wider IT and business objectives.
- Managing the daily operation of the Cyber Operations Centre (SOC), ensuring effective threat detection, analysis, and response to incidents.
- Conducting vulnerability assessments, monitoring system logs, and managing remediation plans in collaboration with IT teams.
- Co-ordinating incident responses, documenting actions, supporting investigations, and ensuring lessons learned are embedded in future practices.
- Assisting with the implementation and maintenance of the Society's cyber security governance framework, policies, and standards.
- Monitoring security tools, technologies, and dashboards to ensure accurate and timely detection of potential threats.
- Working closely with the IT Infrastructure team to ensure that risk management and compliance controls are consistently applied.
- Maintaining awareness of emerging vulnerabilities, zero-day threats, and new technologies to continually enhance the Society's security posture.
- Collaborating with Security Architects to ensure secure design principles are applied to projects and infrastructure upgrades.
- Managing and reviewing third-party security service providers, SOC partnerships, and vendor performance to ensure value and effectiveness.
- Preparing and delivering regular security reports, dashboards, and key risk metrics for the Senior Cyber Security Manager and leadership teams.
- Promoting a culture of cyber awareness by contributing to training programmes, communications, and colleague engagement activities.
- Supporting periodic internal and external audits, ensuring compliance with ISO/IEC 27001 and other regulatory frameworks.
- Providing subject matter expertise during security reviews, change assessments and digital transformation projects.
- Supporting investigations into security events, breaches, or near misses and ensuring timely corrective action is taken.
- Contributing to the development of incident response plans, playbooks, and tabletop exercises to strengthen resilience.
- Liaising with external agencies, partners, and industry peers to share threat intelligence and best practice.
- Continuously identifying opportunities to automate, streamline, and strengthen cyber operations processes.
- Acting as deputy to the Senior Cyber Security Manager when required.

# Our Approach

*Our way of thinking about the purpose of what we do*

## Together we THRIVE...


- **Trustworthy –** we do what we say we'll do and trust others to deliver to the best of their ability
- **Helpful -** we support and challenge each other collaboratively, no matter the role or level.
- **Respectful -** we listen to other views and opinions with consideration and celebrate differences.
- **Inspiring -** we role model what good looks like and lead by example to be better.
- **Valued -** we recognise achievements and appreciate everyone's contributions.
- **Empowered -** we listen and encourage each other to take opportunities.

## Your Approach – *how you will contribute to your team and the Society's ongoing success in this role.*

| | |
|---|---|
| **I will be trustworthy by:** | – Maintaining confidentiality and integrity when managing security incidents.<br>– Demonstrating reliability in managing critical cyber operations and reporting.<br>– Following through on commitments to resolve risks and vulnerabilities.<br>– Building confidence through transparent and honest communication. |
| **I will be helpful by:** | – Supporting IT and business teams to resolve security issues effectively.<br>– Providing clear and constructive advice to improve cyber resilience.<br>– Sharing knowledge and best practice across departments.<br>– Working collaboratively to enhance the Society's overall security posture. |
| **I will be respectful by:** | – Engaging positively with colleagues across all levels of the business.<br>– Respecting diverse perspectives when managing security challenges.<br>– Communicating feedback with professionalism and empathy.<br>– Building respectful relationships with suppliers and partners. |
| **I will inspire others by:** | – Leading by example in promoting cyber security awareness and best practice.<br>– Demonstrating passion and commitment to protecting the organisation.<br>– Encouraging others to adopt a pro-active approach to security.<br>– Inspiring colleagues through visible leadership and technical excellence. |
| **I will value people by:** | – Acknowledging the efforts of colleagues who strengthen our defences.<br>– Recognising improvements and innovations in cyber practices.<br>– Celebrating collaboration and shared success across teams.<br>– Promoting a culture that values learning and continuous improvement. |
| **I will empower others by:** | – Empowering teams to take ownership of local cyber hygiene.<br>– Supporting colleagues to make informed, confident security decisions.<br>– Encouraging innovation in how we detect and respond to threats.<br>– Taking initiative to improve tools, processes, and systems. |