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:	- Leading the Society's cyber security strategy, operations, and governance to protect systems, data, and digital assets, including oversight of the Security Operations Centre (SOC), governance frameworks, threat detection, incident response, and risk mitigation. - Collaborating with IT and business stakeholders to maintain a robust, compliant security posture aligned with evolving threats and regulations.
You'll report to:	- Head of IT and Digital
Your relationships:	- Colleagues within the IT and Digital team. - Colleagues from across the Society which includes our Trading Areas, Community, Membership, Health, Safety & Security, etc. - Executive Leadership / Board Committees (e.g. Risk & Audit Committee) - Suppliers: Oversee third-party monitoring, SOC services, and threat intelligence support. Engage with tool and platform providers for solution evaluation, procurement, and support - Regulatory Authorities / Auditors (e.g., ICO, FCA, external auditors): Respond to audits, submit compliance documentation, and report significant incidents as required. - Industry Forums / ISACs / Cyber Networks: Share intelligence and stay informed on emerging threats and peer responses Industry Peers & Forums: Engage in industry groups to share knowledge and track emerging trends and best practices.
Key role responsibilities:	- A full UK driving licence and access to a vehicle for business use. - This role is subject to DBS clearance.
Your hours:	- 39 hours per week (FTE). - Typical working hours will be Monday – Friday, 8.30am – 5.00pm.

What you'll bring to us:

- Bachelors or Master's degree in Cybersecurity, Computer Science, Information Systems, or a related field, and/or significant experience in Cybersecurity roles.
- A deep understanding of Cybersecurity Frameworks & Standards (e.g. ISO/IEC 27001)
- Previous experience of leading SOC operations, incident response, intrusion detection/prevention (IDS/IPS), Data Loss Prevention (DLP) and threat intelligence.
- Deep knowledge of Network and Infrastructure Security including firewalls, VPNs, proxies, intrusion detection, segmentation, and cloud security controls (e.g., AWS, Azure, GCP).
- Strong knowledge of UK data protection law and regulation, including GDPR.
- Proven experience in Security Strategy Development - Designing and leading enterprise-wide security programs and roadmaps aligned with business goals.
- Experience in multi-disciplinary teams in relation to Cyber Security across multiple stakeholders (IT, Legal, Risk, Trading, 3rd Parties etc).
- An understanding of commercial and financial principles for managing cybersecurity budgets, tools, vendors, and contracts.
- Adaptability to stay ahead of emerging threats, regulatory changes, and technological advancements.
- Networking expertise to harness best practices and industry intelligence on evolving threats.
- Communication skills to translate technical risks for executives and boards, influencing key decisions.
- Leadership and mentoring experience in developing high-performing cyber teams.
- Influencing skills to engage colleagues across the Society and gain buy-in for security initiatives.

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:

- Leading the strategic development and execution of the Society's cyber security vision, roadmap, and policies.
- Managing and providing direction to the cyber security team.
- Establishing, operating, and continuously improve the Society's Cyber Operations Centre (SOC) to ensure 24/7 threat detection, monitoring, and incident response.
- Developing and implementing the Society's cyber security governance framework, including policies, standards, and procedures.
- Overseeing cyber threat intelligence, vulnerability management, and threat-hunting activities.
- Ensuring timely and effective response to security incidents, coordinating investigation, remediation, and post-incident reviews.
- Leading the assessment and management of cyber risks across the Society's digital and technology estate.
- Ensuring compliance to all audit actions continually evolving our security technology, policies and processes.
- Maintaining oversight of the Society's security architecture, ensuring solutions are secure by design and aligned with best practices.
- Ensuring compliance with relevant regulatory requirements (e.g., ISO 27001) and lead audit readiness activities.
- Partnering with IT, Legal, Compliance, Risk, and third parties to ensure a coordinated and effective security posture across the Society.
- Driving security awareness and training initiatives across the Society to foster a strong security culture.
- Monitoring and reporting on cyber security KPIs, risk metrics, and SOC performance to executive leadership and governance bodies.
- Providing expert advice and challenge on major IT and digital transformation programmes to ensure cyber security is embedded from the outset.
- Evaluating and managing third-party vendors and tools that support cyber operations and governance.
- Staying current with the evolving threat landscape, emerging technologies, and industry trends to proactively enhance the Society's security posture

Role Behaviours

The qualities we expect colleagues in this role to demonstrate

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:	- Leading the Society's cyber security vision, roadmap, and strategic policy execution. - Maintaining oversight of secure-by-design architecture aligned to industry practices. - Ensuring compliance with ISO 27001 and all applicable regulatory requirements. - Providing expert assurance and challenge to major digital transformation initiatives.
I will be helpful by:	- Partnering with IT, Legal, and Risk teams to strengthen security posture. - Driving security awareness and training to embed an organisational security culture. - Providing timely expert advice to stakeholders on cyber risks and controls. - Supporting teams with guidance to resolve vulnerabilities and mitigate threats.
I will be respectful by:	- Coordinating incident responses with clear and collaborative communication. - Ensuring security measures respect business priorities while protecting critical assets. - Working closely with external partners to deliver shared security objectives respectfully. - Balancing technical controls with user experience and operational needs.
I will inspire others by:	- Championing proactive threat-hunting and intelligence-led security improvements. - Leading SOC operations to deliver world-class monitoring and rapid incident response. - Encouraging approaches to cyber defence through technologies and practices. - Promoting continuous improvement and excellence in cyber security team performance.
I will value people by:	- Establishing and evolving a cyber governance framework, policies, and procedures. - Overseeing vulnerability programmes to reduce organisational exposure to threats. - Delivering concise, actionable cyber risk and KPI reports to leadership. - Managing third-party security vendors to ensure service quality and compliance.
I will empower others by:	- Directing the cyber security team to deliver against strategic objectives. - Driving continuous enhancement of SOC capabilities for 24/7 threat detection. - Leading cyber risk assessments to guide executive decisions and investments. - Staying ahead of threats by tracking industry trends and adapting defences.

Role Behaviours

The qualities we expect colleagues in this role to demonstrate

Together@ Lincolnshire Co-op

Your behaviours

Adhering to Principles and Values – responding suitably to values-led decisions

Presenting and Communicating Information – translating information appropriately

Relating and Networking – sharing knowledge to develop and learn from others

Working with People – building a strong and adaptable team

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

I will adhere to the principles and values of the Society by:	- Being honest, transparent and consistent in all actions and communications. - Treating others with dignity and respect, valuing their diversity and different perspectives. - Listening actively and consider the opinions of others. - Taking accountability for my actions and decisions. - Fostering a spirit of teamwork, co-operation and positive relationships.
I will present and communicate information clearly by:	- Tailoring my communication to the level of understanding and background of the audience. - Paying close attention to others when they speak. - Providing examples to illustrate complex concepts to make my message more relatable. - Encouraging feedback and questions from colleagues to clarify understanding.
I will build a network of customers and colleagues by:	- Offering value to my network by sharing relevant insights, information, or resources. - Fostering genuine relationships by demonstrating authenticity and integrity in my interactions.
I will work collaboratively with my colleagues by:	- Demonstrating an interest in and understanding of others. - Recognising and rewarding the contribution of others. - Listening and consulting with others and communicating appropriately. - Supporting and caring for colleagues. - Developing and openly communicating self-insight such as an awareness of own strengths and weaknesses.