Head of Cyber Security

> Finance > Financial Services

What's it all about

The Head of Cyber Security is accountable for NHG Digital's cyber security domain, ensuring that digital services, systems, suppliers, data flows and operational environments are protected through clear security strategy, standards, controls, monitoring, assurance and incident response.

The role owns cyber security policy, cyber risk position, control assurance and specialist security judgement. It helps protect residents, staff, services, data and public trust by making cyber risk visible, understood and managed through practical controls and clear evidence. It ensures product, architecture, engineering, transition, operations, data, supplier and governance activity is supported by clear security requirements, proportionate controls, evidence-based assurance and timely escalation of unresolved cyber risk.

How you'll make a difference

You will protect NHG's residents, staff, services and reputation by ensuring cyber risk is understood, governed and managed as a core business risk, not just a technical issue. You will help NHG maintain trust in the digital services that residents and colleagues rely on every day.

You will strengthen resilience by making sure security requirements are embedded early in product discovery, architecture, DevOps delivery, supplier management, transition, live operation and continuous improvement. Your success will be measured through improved security posture, reduced exposure, stronger assurance evidence, effective incident readiness, better security awareness and clear cyber-risk reporting.

You will work visibly and collaboratively with Products, Architecture, DevOps, Digital Operations, Customer Operations, Digital Governance, Data and Corporate Reporting, service owners, suppliers and senior leaders, maintaining a minimum of two days per week onsite to build trust, support timely decisions, improve security behaviours and provide calm, credible leadership during security concerns or incidents.

How you'll do it

- You will establish and maintain NHG Digital's cyber security strategy, roadmap, policy content, standards and control framework for the security domain, ensuring they are proportionate to NHG's risk appetite, operating model, regulatory context, supplier landscape and changing threat environment.

- You will own specialist cyber security assurance across products, platforms, integrations, infrastructure, suppliers, identity, access, privileged access, perimeter controls, vulnerability management, monitoring, incident response and recovery. You will define and assure expectations for identity, access and privileged-access controls, ensuring access risk is visible, reviewed and evidenced across internal users, suppliers, administrators and service accounts. You will ensure cyber requirements are clear, evidenced, tested and escalated where risk cannot be resolved within normal delivery or operational routes.

- You will work with the Head of Digital Products to ensure product discovery, service design, adoption and benefits decisions consider security implications, resident and staff trust, privacy expectations, identity, access, fraud, supplier exposure and operational resilience from the outset. You will support early product and service-design decisions where cyber risk, identity, customer data, supplier connectivity, fraud risk, monitoring or resilience could affect resident or staff trust.

- You will work with the Head of Digital Architecture to ensure solution designs, architecture patterns, domain boundaries, integrations, cloud and platform decisions, AI-enabled services and supplier proposals include appropriate security requirements, threat considerations, control design, monitoring expectations and residual-risk visibility.

- You will work with the Head of DevOps to embed secure engineering practice, including secure coding, configuration control, environment separation, vulnerability remediation, secrets management, test evidence, release assurance and deployment controls. DevOps will own engineering execution; you will own the cyber requirements, assurance position and escalation of unresolved security risk.

- You will work with the Director of Digital Operations and Head of Digital Operations to ensure live operational practice sustains agreed cyber controls for patching, vulnerability response, monitoring, privileged access, backup and recovery, incident response, operational resilience and supplier-operated services. Operations will own live operational control; you will own the cyber risk position, assurance evidence and specialist challenge.

- You will work with the Programme and Transition Manager to ensure transition readiness includes cyber assurance evidence, security test outcomes, access controls, monitoring arrangements, incident-response expectations, supplier obligations, residual-risk decisions and security-related go/no-go criteria before a service moves into production.

- You will work with Digital Governance to ensure cyber decisions, risks, exceptions, residual-risk acceptances, policy compliance, audit actions, supplier control evidence and assurance outcomes are visible, controlled and auditable within NHG's governance framework. You will provide specialist advice on residual cyber risk, ensuring unresolved risks are clearly described, evidenced, escalated and accepted only through the agreed governance route. Governance will own the governance route and audit trail; you will own the cyber content, risk assessment and specialist assurance judgement.

- You will work with Data and Corporate Reporting to protect data confidentiality, integrity and availability, ensuring data flows, reporting, retention, analytics, AI-enabled services and corporate information assets are assessed for cyber risk and protected through appropriate controls.

- You will lead cyber monitoring, threat awareness, incident preparation and major cyber incident response coordination, ensuring NHG has clear playbooks, escalation routes, communication principles, evidence capture and recovery expectations. You will provide clear, proportionate advice to senior leaders on the impact, likelihood, response options and residual risk associated with cyber threats and incidents.

- You will hold suppliers and managed service partners to account for cyber obligations, including security requirements, access controls, assurance evidence, incident notification, vulnerability remediation, penetration testing, contractual controls, exit risk and ongoing compliance with NHG's security expectations.

- You will build cyber security awareness, capability and confidence across NHG Digital, helping technical and non-technical colleagues understand their role in protecting residents, staff, data, services and public value. You will challenge weak practice constructively and escalate material risks through the agreed governance route.

- You will follow all relevant NHG and statutory policies and procedures, including health and safety, financial regulations, procurement, data protection, records management, accessibility, cyber security, business continuity, incident management, supplier management and responsible AI requirements.

All about you

You bring strong experience leading cyber security, information security, security operations, cyber risk, security assurance or resilience in a complex, regulated or similarly accountable environment where sensitive data, essential services, supplier dependencies and public trust all matter.

You can operate confidently between strategic risk and technical detail: able to advise senior leaders on cyber risk appetite, assurance and incident decisions, while also understanding the practical controls needed across identity, access, monitoring, vulnerability management, cloud, platforms, suppliers, integrations and live operations.

You are calm, credible and proportionate. You understand that effective cyber security is not about saying no to change; it is about enabling digital services to be designed, delivered, operated and improved safely, with clear evidence, informed risk decisions and strong accountability.

You are visible, collaborative and values-led, able to build trust with technical teams, service owners, suppliers, governance forums and senior leaders while constructively challenging practice that creates avoidable cyber, operational, data or service risk.

Our values

We succeed together
By working as one and respecting diverse perspectives, we support each other to consistently deliver better outcomes for our residents and communities.

We keep our word
We do what we say we will do, and act with integrity and ownership to build trust and provide the high-quality service people expect from us.

We do better every day
We are always looking for better ways to work and raising standards and strengthening communities through continuous improvement.

For each value, we've created example behaviours to help you understand our expectations in more detail. This role is at Manager level.

Essential knowledge, experience and skills

Pending confirmation of legislative changes, this role may require a qualification to demonstrate competence. If not already qualified, there may be an expectation to study towards a professional qualification.

- Substantial experience leading cyber security, information security, security operations, cyber risk, security assurance or resilience within a complex, regulated or similarly accountable environment.
- Strong knowledge of cyber security strategy, policy, standards, controls, risk management, assurance, monitoring, vulnerability management, incident response and recovery.
- Proven ability to define and maintain proportionate cyber security controls across identity, access, privileged access, perimeter security, cloud, platforms, infrastructure, applications, integrations, suppliers and live operational environments.
- Experience embedding security requirements into product discovery, architecture, DevOps delivery, supplier management, service transition, change control and live operations.
- Ability to assess and explain cyber risk, control gaps, residual-risk options and assurance evidence clearly to senior leaders, technical specialists, service owners and non-technical stakeholders.
- Experience leading or coordinating cyber incident preparation and response, including playbooks, escalation routes, evidence capture, communication principles, recovery expectations and lessons learned.

- Good understanding of data protection, privacy, records management, business continuity, operational resilience, supplier assurance, responsible AI, auditability and regulatory expectations in a digital service environment.

- Experience holding suppliers and managed service partners to account for security obligations, assurance evidence, access controls, incident notification, vulnerability remediation, penetration testing, contractual controls and ongoing compliance.

- Strong communication and influencing skills, with the ability to promote security awareness, advise senior leaders, challenge constructively and translate technical security issues into practical business risk decisions.

- Visible, values-led leadership style, with the ability to build capability, support teams under pressure, escalate appropriately and create an inclusive, accountable and security-aware culture.