JOB DESCRIPTION

Job Title	**Director, Cyber Security**		
Reports to	**Chief Digital and Information Officer**		
Department	**Technology**		
Job Family	**Business Services**	**Level**	**5**

About the School

At London Business School, we strive to have a profound impact on the way the world does business and the way business impacts the world. Our departments work hard to ensure that we are continually delivering a world-class service, academic excellence and that our course offering maintains our place as a leading business school.

With thought-leading faculty and dynamic learning solutions, we empower both businesses and individuals by offering a transformational learning experience that will broaden their professional knowledge and global mindset. As well as offering postgraduate courses for the business leaders of the future, we run open and customised executive courses for professionals and corporate clients that help leaders identify the future focus and strategic direction of their businesses.

With London in our hearts, we draw from its status as a financial, entrepreneurial and cultural hub to attract a diverse range of students and faculty, creating an abundance of opportunities to network with industry experts and alumni worldwide.

About the Department

The LBS Technology department is responsible for delivering and supporting all digital technology solutions required for the effective running of London Business School.

We provide specialist capability in Service Delivery, Software Development, Digital Solutions Delivery, Teaching and Learning Technology, Platform integration, Data Management, Cyber Security, Project Delivery, Business Change and Enterprise Architecture.

Cyber security transformation is a key focus area, and a step-change in approach and security posture is required to ensure that flexible solutions are built with security embedded by design to reduce the risk of business impacting security incidents. The School is determined to offer demonstrable cyber security intent, compliance and structured progress over a sustained period.

Job purpose

The Director, Cyber Security will serve as the primary advocate for the School's information security posture, collaborating across the organisation to protect data assets, manage risks, and lead the Cyber Security Team in implementing a comprehensive information security program. You will provide strategic leadership in cyber security governance, risk management, compliance, and incident response.

As a member of the Technology Senior Management team the Director, Cyber Security will:

- Influence technology leaders and data privacy leaders to ensure the priority of Cyber Security is prioritised across the School.
- Recruit, lead, develop and motivate the Cyber Security Team within the Technology Department.
- Through a programme of initiatives for London Business School, and measured against the NIST Framework:
    - Deliver foundational security processes and services to raise the bar for cyber security and offer visible and demonstrable improvements.
    - Support the delivery of secure platforms and services to reduce technical debt, improve security posture, and provide confidence in technology.
    - Develop cyber security analytics and response capability to ensure data-driven, risk-based decisions are facilitated and lessons are continuously learned.
    - Ensure pragmatic and proportionate protection is applied to all LBS data assets and systems according to the level of risk.
    - Develop cyber security resilience via robust incident response capabilities.
    - Work towards attaining and maintaining ISO27001 certification for London Business School.
- Influence the work of the Project Managers leading delivery streams which support the Cyber Security Programme initiatives, creating a single consolidated view on progress.
- Be the senior point of escalation for any Cyber Security Incident at the School.
- Report on a regular basis to Audit and Risk Committee on the progress and health of the schools Cyber Security posture.
- Manage external partners to ensure progress is on track and demonstrable improvement in our security posture is evidenced.
- Act as the escalation route for any emerging programme risks and issues are brought to the attention of the sponsor (CDIO).

Key Areas of accountability and Key Performance Indicators

Key areas of accountability:

Key Areas of accountability and Key Performance Indicators

Cyber Security Strategy & Leadership

- Develop and implement an enterprise-wide cyber security strategy aligned with the School's technology and organisational goals.
- Provide leadership on information security policies, standards, and guidelines, ensuring they are embedded across all initiatives.
- Engage with senior leadership to promote the importance of cyber security and ensure alignment with broader organisational priorities.
- Be an active contributor to the development of the Technology department, attending regular Technology SMT meetings.

Risk Management & Compliance

- Develop and maintain a risk management framework that identifies, evaluates, and addresses information security risks.
- Lead efforts to attain and maintain compliance with information security standards, including ISO27001 certification, and other relevant regulatory and legal requirements.
- Establish key metrics to monitor the effectiveness of the information security program and report regularly to the Audit and Risk Committee on the school's cyber security posture.

Security Operations & Incident Response

- Oversee and mature the School's security operations, including threat monitoring, vulnerability management, and incident response.
- Develop and lead a robust incident response process, acting as the primary point of escalation for cyber security incidents, ensuring that appropriate stakeholders are informed.
- Build and enhance the organisation’s cyber resilience, working to reduce response time and improve recovery capabilities.

Governance, Risk, and Compliance (GRC)

- Lead Governance, Risk, and Compliance (GRC) efforts within information security, ensuring alignment with the School's overall GRC activities.
- Collaborate with relevant teams to integrate security into the School's project and service delivery processes, ensuring compliance is achieved by design.

Stakeholder Engagement & Collaboration

Key Areas of accountability and Key Performance Indicators

- Act as the primary point of contact for cyber security matters and partner with business leaders, technology stakeholders, and external partners to support secure outcomes.
- Influence and educate stakeholders at all levels, fostering a security-aware culture that prioritises safeguarding sensitive information.

People Leadership & Development

- Lead, motivate, and develop a team of Cyber Security professionals, promoting a culture of collaboration, inclusion, and continuous learning.
- Build capability in both Cyber Security Operations and Governance, Risk, and Compliance (GRC) areas.
- Recruit, mentor, and manage team members, ensuring they have the skills and training necessary to excel in their roles.

Supplier & Partner Management

- Manage external partners to ensure they contribute effectively to the School's security posture, including security operations providers and those assisting with compliance and certification.
- Evaluate and oversee the work delivered by third-party suppliers, ensuring adherence to service level agreements.

KPIs:

- Successful implementation of foundational security measures to reduce risk.
- Achievement and maintenance of ISO27001 certification.
- Improvement in security incident response times and reduction in business impact.
- Positive feedback from stakeholders on the effectiveness of cyber security initiatives.
- Successful integration of security into organisational processes and projects.
- Contribution to cross-School compliance with regulations and legislation.

Knowledge/Qualifications/Skills/Experience required

Knowledge/Qualifications Required:

- Proven experience leading a cyber security function in a medium to large organisation.
- Strong understanding of Governance, Risk, and Compliance (GRC) related to information security.
- Track record of developing and implementing information security strategies and programs.
- Experience managing ISO27001 compliance and working within regulatory frameworks.
- Strong interpersonal skills, with the ability to communicate complex information clearly and influence stakeholders at all levels.

Skills

- Experience of building, motivating, and leading delivery teams and maintaining a supportive and collaborative working environment within the team that promotes equality, diversity and inclusion
- Ability to influence and persuade others to take a specific course of action when there is no direct line of command or control and direct others to undertake tasks.
- Excellent written and verbal communication skills with the ability to present complex information clearly and effectively in appropriate styles at all levels.
- Strong interpersonal skills with the ability to establish positive working relationships and influence people at all levels within the organisation including a challenging customer base.

Resources including team management

Staff	Leading a team of 4, including service operations analysts and GRC analysts, as well as managing partnerships with delivery partners for certification and security operations.
Budgets	Approval level - up to £25k
Date Updated	5 November 2024