M8 Solutions

DELIVERING TECHNICITY WITH INTEGRITY

Chief Information Security Officer as a Service (CISOaaS)

Strategic CISOaaS Leadership Delivered by M8 Solutions

WHY M8 SOLUTIONS FOR CISOaaS?

Strategic Cyber Security strategy, leadership and protection, delivered by experts without the overheads of in-house resources.

THE IMPORTANCE:

The role of a CISO is pivotal in safeguarding an organisation's information assets and aligning security strategies with business objectives. Effective leadership is critical to staying ahead of modern threats and maintaining regulatory compliance. M8 Solutions' CISOaaS provides access to seasoned Cyber Security leadership when you need it most - offering the expertise, insight, and strategic direction to protect your organisation and support your long-term success.

THE M8 SOLUTIONS DIFFERENCE:

Our service delivers executive-level guidance without the commitment of a full-time hire, integrating seamlessly with your team to enhance your organisation's security posture. We offer a comprehensive suite of services tailored to your organisation's specific needs, ensuring resilience against evolving cyber threats and alignment with your strategic goals. The following pages outline the key areas a CISO-as-a-Service can cover - with every aspect fully customisable to suit your organisation's size, and existing capabilities.

> ***"Security is not optional - it is essential. In a world where threat actors move fast, your defences need to move faster."***

Tom Duffell,
Cyber Security Specialist.
M8 Solutions

OUR PROPOSED APPROACH TAILORED TO YOUR NEEDS:

STRATEGIC PLANNING AND POLICY DEVELOPMENT

- Security gap analysis using M8 Solutions’ Cyber Security Diagnostic Programme, highlighting your critical areas of focus
- Develop and implement comprehensive Cyber Security strategies and policies aligned with your organisation's goals, national Cyber Security initiatives and best practices, including both on-premises, Cloud Security and hybrid strategies helping to mitigate the cyber risks as identified in HM Governments National Risk Register,
- Ensure that security policies align with relevant regulations and standards.
- Regularly review and update security policies to address new threats and vulnerabilities.
- Guidance on the adoption of relevant industry related Cyber Security frameworks.
- Support governance, risk and compliance, initiatives and activities.

RISK ASSESSMENT AND MANAGEMENT

- Conduct information security risk assessments to identify and quantify potential vulnerabilities.
- Provide reports on emerging cyber threats to your organisation, including threat alerts.
- Manage vulnerability assessments and Penetration Testing.
- Develop risk management plans to mitigate identified risks and implement security controls.
- Monitor and review risk management processes to ensure their effectiveness.

TRAINING AND AWARENESS

- Develop and deliver training programmes to educate employees about Cyber Security best practices.
- Promote security awareness across the organisation through campaigns and initiatives, including phishing simulations to create a Cyber Security culture.
- Ensure that employees are aware of their roles and responsibilities in maintaining security.

INCIDENT RESPONSE AND MANAGEMENT

- Develop and maintain an incident response plan to handle security breaches and cyber attacks.
- Disaster recovery and business continuity planning to ensure uninterrupted services.
- Design and deliver incident response exercises to increase preparedness.
- Lead the response efforts during security incidents to minimise impact and ensure quick recovery.
- Conduct post-incident analysis to identify lessons learned and improve future response strategies.
- Assist with incident reporting to the relevant regulatory bodies, such as the Information Commissioner's Office (ICO).

SECURITY OPERATIONS

- Oversee the day-to-day operations of the Cyber Security programme, including security monitoring and responding to security alerts.
- Guidance on security operations architectures and practices, such as a Zero Trust architecture models and a secure by design approach, encryption and key management solutions and Identity and Access Management (IAM) frameworks to protect your organisations data.
- Ensure the implementation and maintenance of security tools and technologies.
- Manage security-related projects and initiatives.

LEADERSHIP AND COLLABORATION

- Provide C-suite advisory services, ensuring that executives, board members, and senior leadership teams understand cyber risks and regulatory obligations maximising your strategic security investments.
- Translate technical security challenges into actionable business intelligence, enabling informed decision-making.
- Ensure Cyber Security is aligned with business objectives, financial goals, and digital transformation initiatives.
- Deliver regular Cyber Security briefings, risk reports, and board-level security insights to ensure leadership prioritises security as a business-critical function.
- Guide leadership teams through crisis management, regulatory compliance changes, and emerging cyber threats.
- Represent the organisation in discussions with regulators, government bodies, and industry groups, ensuring alignment with security best practices.
- Act as a public-facing Cyber Security representative, advocating for strong security policies and engaging in industry discussions on evolving cyber threats.

EMERGING TECHNOLOGIES AND TRENDS

- Stay informed about emerging technologies and trends in Cyber Security, such as the use of Artificial Intelligence (AI) and Quantum Computing.
- Assess the potential impact of new technologies on the organisation's security posture.
- Recommend and implement innovative security solutions to address evolving threats, including AI.
- Horizon scanning of new Cyber Security products and services.

VENDOR AND THIRD-PARTY MANAGEMENT

- Evaluate and select security vendors and third-party service providers.
- Ensure that third-party security practices align with the organisation's security standards to secure the supply chain.
- Monitor and manage third-party and supply chain security risks.
- Provide security due diligence assessments on products and services procured.

ORGANISATION REPORTING AND METRICS

- Regular touchpoints, updates and regular security posture reports.
- Develop and present regular reports on the status of the information security programme to senior management and the C-suite.
- Track and analyse security metrics to measure the effectiveness of security initiatives.
- Use metrics to identify areas for improvement and drive continuous enhancement of the programme.

COMPLIANCE AND AUDIT

- Ensure compliance with industry standards, regulations, and internal policies.
- Collaborate with internal and external auditors to review security practices and address findings.
- Maintain compliance documentation and evidence of compliance activities.

BUDGETING AND RESOURCE ALLOCATION

- Manage the Cyber Security budget and allocate resources effectively.
- Identify and prioritise investments in security technologies and initiatives.
- Ensure efficient use of resources to increase the impact of security efforts and ensure maximum ROI.

SECURE YOUR ORGANISATION'S FUTURE WITH M8 SOLUTIONS

Effective Cyber Security safeguards, reputation, compliance, and continuity.

Partnering with M8 Solutions for CISOaaS equips your organisation with the strategic leadership necessary to navigate the ever-evolving cyber threat landscape. Our comprehensive approach ensures your information assets are protected, compliance requirements are met, and your business objectives are supported by a robust security framework. This service provides your organisation with a combination of technical expertise, strategic thinking, and strong leadership to navigate the complex and ever-changing landscape of Cyber Security.

Contact us today to learn how M8 Solutions can enhance your organisation's Cyber Security posture and provide the leadership needed to thrive in today's digital landscape.

> ***"M8 Solutions' CISOaaS helps to create a secure environment that protects your sensitive information, maintains continuity, and fosters trust among stakeholders."***

Tracy Scriven,
Chief Executive Officer.
M8 Solutions

TESTIMONIAL

David Tudor

Head of Service Delivery

NHS
University Hospitals of North Midlands
NHS Trust

"Having recognised a potential challenge due to the loss of a key member of the Cyber Team, I approached M8 Solutions to understand what they could provide.

Tracy introduced me to the Cyber team, she described the team as one which was born from a military background with skills that far surpass that of your average Cyber Security partner. I find the teamwork with M8 Solutions to be unique. I find the individual responsible for delivering our CISOaaS to be exemplary and completely focused on what the Trust needs, he is not led by any supplier sales strategy. His knowledge, ability and flexibility to go above and beyond has been second to none.

I am thoroughly satisfied with the solution provided and would not hesitate in recommending."

Neil Godfrey

Deputy Director of Digital

NHS
East of England
Ambulance Service
NHS Trust

The M8 Solutions team demonstrated deep technical expertise, a clear understanding of NHS operational realities, and an ability to translate complex cyber scenarios into meaningful, actionable learning.

M8 Solutions

DELIVERING TECHNICITY WITH INTEGRITY

☎ 01782 634 993

✉ info@m8solutions.co.uk

🌐 www.m8solutions.co.uk