CASE STUDY

SECURITY WAS THE BUSINESS ENABLER

Medicare Network
More intelligent, More Secure

How an Industry Regulator Recovered from a Data Breach

COMPANY PROFILE

Medicare Network is a niche, forward-thinking cybersecurity and risk management company dedicated to solving the healthcare and pharmaceutical industries most important cybersecurity challenges.

Providing proven experience, expertise and individuals who share the passion in preventing the most sophisticated and targeted cyber-attacks to critical infrastructure and life-critical medical technologies.

We are a vendor agnostic company that carefully identify and select world-class innovative cybersecurity solutions that leverage the latest cloud, AI and machine learning capabilities. To intelligently detect and respond to any potential cyber threats to IT, and Operational Technology (OT) systems and infrastructures.

We deliver security transformation and driving better value in the age of digitalisation!

AT A GLANCE

- Government-backed regulator needed to address multiple Information Security issues
- Data breach exposed much deeper challenges through the discovery process
- Absence of Information Security framework threatened both security and compliance
- 'People first' approach successfully embedded security awareness from front desk to Boardroom
- Security expertise became fundamental to client's ongoing IT transformation
- Improved accountability and reporting, suitable for scrutiny by independent Governance, Risk and Audit oversight committee

THE CLIENT

An industry regulator, created by Act of Parliament and closely connected to the Government, **this client represents one of the nation's most respected professions, and handles extremely sensitive personal and professional data relating to drugs and medicines.** Compliance, security and reputational integrity are therefore critical to both its day-to-day operations and its continuous improvement programmes.

THE CHALLENGE

An initial data breach had immediately raised four further issues:

- The protection of individuals' identities during professional Fitness to Practice Committee inquiries
- The need to collaborate with the ICO to complete the process of documenting and responding to the breach
- The need for prompt root-cause analysis of the breach, and swift technical and organisational action to prevent it happening again
- Increased Government and industry pressure to fully understand the organisation's overall security posture, take corrective action, and ensure ongoing compliance and assurance

But even in the face of such urgency, a 'quick fix' was not enough. Although rapid remediation of the data breach was of course essential, the issues behind such a breach - and many other potential Information Security issues - in a highly knowledge-driven environment, dependent on intensive human input, would be fuelled by staff and process error at all levels, not just by technical security shortcomings.

As explained by a member of the Executive Team and the Interim Executive, who was also the Head of Information Security,

> "We didn't need security to be done to us or done for us – we needed it to be done with us, involving everyone from the receptionist to the CEO."

THE SOLUTION

After identifying and remediating the data breach, Medicare Network prepared and supported senior management to collaborate fully with the ICO on the incident's administration and closure.

Then, Medicare Network put in a place a comprehensive audit of **people, processes, technology** and **physical environments** – in order, to identify the full extent of vulnerabilities and risks, working closely with the organisation's Executive Team to produce a programme of works to deliver:

More secure behaviours from all employees

Security and data loss education and knowledge transfer sessions at all levels, from the front desk to the Boardroom, helping to prevent the need for costly breach clean-ups.

A clear, step-by-step improvement plan

'Hand-holding' through ten priority security enhancements and working hand-in-glove with facilities, and IT departments to implement, including (amongst others); CCTV coverage, document destruction procedures, secure printing, mobile device management, encryption, vulnerability management, supply chain security, online payment security (PCI-DSS) and security policies, standards and strategy.

Industry-recognised security infrastructure

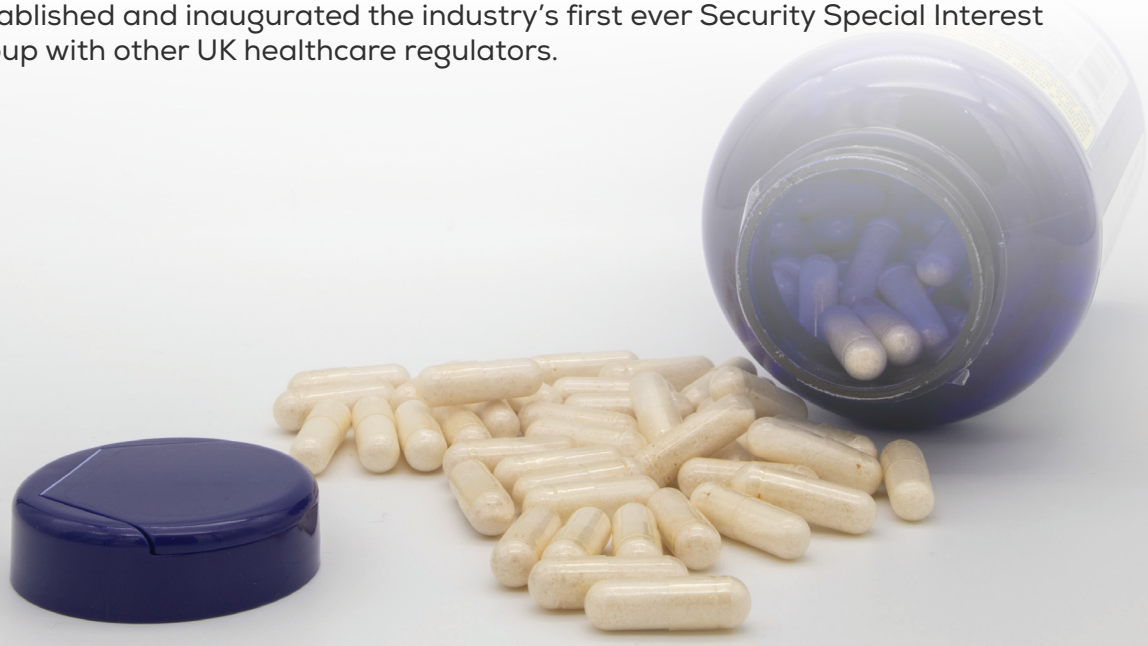
Established an ISO27001 Information Security Management System (ISMS and a clear roadmap to compliance and, potentially required in the future, certification.

De-risked supplier relationships

Reduced risk in the supply chain in both directions, by adding security statements and requirements, ensuring the security posture of suppliers was significantly improved, and by enforcing third-party contractual obligations.

Critical industry intelligence

Established and inaugurated the industry's first ever Security Special Interest Group with other UK healthcare regulators.



OUTCOMES AND RESULTS

Quite apart from the extensive improvements to the organisation's security posture – its readiness to identify and deal with security issues – Medicare Network's relationship with the client has left a legacy of security awareness and privacy.

Security is now something to be discussed openly, at all levels (not just by the C-Level), with accountability established across all business areas (not just IT).

And if any evidence were needed that security is not just a box-ticking exercise, but is at the very heart of business success, Medicare Network was also selected to manage both day-to-day operational activities within the organisation, and to lead several digital transformation workstreams.

PASSIONATE PEOPLE, DEDICATED TO YOUR SUCCESS!

The changing landscape and constant evolution of cyber threats means that protection-levels and education for staff, is a continuing process for every business. Medicare Network's primary focus is providing integrated security transformation services and solutions to healthcare providers and pharmaceutical organisations of all sizes to prevent, detect and recover from a security incident or breach.

FOR MORE INFORMATION

- UK/EMEA +44 (203) 355-3785 - US +1 (702) 605-4601 - clientservices@mednetsec.com
- Mortlake Business Centre | 20 Mortlake High Street | London | SW14 8JN | United Kingdom
- www.mednetsec.com