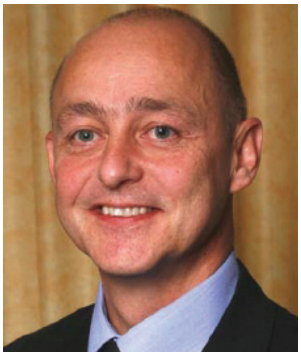
Financial Services Case Study

Reducing the risk of confidential data loss



The client

Generic Financial Management plc is a well established firm of chartered financial planners based in Hertfordshire. The company provides a personal service to its clients, advising on wealth matters.

The issue

The Financial Services Authority's (now the Financial Conduct Authority) 2008 report on Data Security in Financial Services focused on the issues surrounding client data losses through theft of laptops and memory sticks.

Knowing that any breaches of Personal Identifiable Information (PII) within the company would result in fines by the regulator, the senior management team took seriously their responsibility for the security of sensitive clients data and Octree was asked to review the company's IT systems, processes and security.

Octree's approach

Suitable for businesses with multiple servers and a complex IT infrastructure. ProfessionalPlus provides 24/7 support covering everything, from networks and servers to mobile devices to security appliances.

Like many financial services companies, Generic Financial Management had become totally reliant on the use of technology, from office-based servers and PCs to laptops, and the use of CDs and USB memory sticks to transfer information. All employees had access to the Internet and email was widely used to communicate with clients and suppliers.

We conducted an audit of the company's IT systems and infrastructure using a detailed questionnaire that Octree has developed to accurately assess the level of compliance with the FSA's data security guidelines and accepted industry best practice. The methodology ensured that fundamental weaknesses in IT security systems and procedures were quickly identified.

Based on the findings of the audit, we implemented a range of measures to improve data security, including:

- Full disk encryption of company laptops, providing protection against unauthorised access to data in the event of hardware being lost or stolen.
- Web filtering to control employee access to inappropriate or non-work related websites and to protect PCs from web-based malware.
- Email filtering to protect PCs against phishing email, spam, email-borne viruses and malware. It also ensures that inappropriate or defamatory material is blocked.
- Endpoint security on desktops and server with anti-virus, anti-malware and proactive threat protection (IPS).
- Patch and vulnerability remediation to keep software up to date.
- A managed firewall and VPN offering secure remote access for mobile users.

Managing Director of Generic Financial Management says: "Octree's work ensured we are in much better shape to handle our clients' information securely, it's given the entire company an incredible boost in confidence. We also have peace of mind knowing that Octree now manages our IT services. Server services, storage and back up is routinely monitored and we have access to remote support in the event of any problems."

OCTREE

For further information contact:
security@octree.co.uk
08456 17 18 19
www.octree.co.uk