THORNTONS

Market Sector: Legal

Established in 1857 Thorntons Law has grown to become one of Scotland's leading and largest law firms with 29 partners and over 270 staff working from a network of offices including Dundee, Perth, Arbroath, Forfar and Edinburgh. The company provides the complete range of legal services for businesses and individuals covering all areas of corporate law through to residential property purchases.

THE CHALLENGE

Due to the specialist nature of their work, Thornton's lawyers are frequently required to work from any of the firm's offices as well as at client premises to finalise important contracts and agreements, which means needing to have flexible and secure access to case files at all times.

Thornton's have invested heavily in providing the necessary IT infrastructure to support this critical business requirement and are continually reviewing their corporate network to ensure that the system keeps pace with the evolving needs of the business and developments in high speed technology as well as ensuring it meets the latest security compliance standards required to protect client information.

Following a review of the system, Thornton's Director of IT, Sarah Blair identified several areas of the system that were causing concerns and support issues.

In particular it was becoming very time consuming to meet the needs of the growing number of staff who wanted to work more flexibly by working from home at weekends and holiday periods. In addition, users were finding the old system cumbersome and limiting their ability to access the full range of functionality they would have when they are in the office.

Thornton's approached a number of potential companies in the region for advice and guidance on how to upgrade their existing remote access system before deciding to work with Stockton-On-Tees based Sapphire* to deliver what was needed.

THE SOLUTION

Having carefully assessed Thornton's existing remote access system and considered the company's long term requirements, Sapphire identified the need for a more reliable and flexible VPN technology combined with a sophisticated firewall that was capable of fine- grained traffic management to protect the network from un-authorised access and data leakage.

Sapphire also regarded the need for a strong authentication technology to control access to the critical servers and confidential client files as a critical element of the recommended solution. As a legal services company Thornton's reputation could be seriously damaged if client files were compromised through a weak access control policy as well as potentially finding them in breach of the latest data protection legislation.

The solution recommended and installed for Thornton's was based on a Microsoft Intelligent Application Gateway (IAG) combined with the Swivel, tokenless, multi-factor authentication system and a Stone gate Firewall appliance.

Microsoft IAG is a browser based SSL VPN which enables Thornton's remote users to securely link to the company's data centre via any Internet connection without the need for any special client software to be installed on the user's PC or laptop, reducing the need for IT support to configure individual's devices or install dedicated equipment in the users' homes. Combined with a Stonesoft Stonegate firewall the system enables Thornton's to enforce a specified user access policy to control and monitor all traffic through the network gateway.

Swivel provides a second layer of user authentication in addition to the normal username and password logon procedure, which is a standard feature of the IAG technology.

Before Thornton's users are allowed access to the client files and network applications they must enter a unique one-time-code generated by the Swivel technology. The OTC is generated through the combination of a random security string, sent to the browser or a mobile phone, together with the user's registered PIN code. This simple process ensures that only authorised personnel are able to access the system and protects user identities from being intercepted or stolen, without the need for an expensive token-based system typically needed with other strong authentication technologies.

DELIVERY

The staged implementation of the new remote access system was planned and implemented by Sapphire together with Thornton's IT team and support from Swivel's technical consultants to minimise the disruption to the company's core operations and to ensure a smooth transition from the old system. The whole process was completed on time and on budget in accordance with the agreed implementation plan.

RETURN ON INVESTMENT

Since the completion of the system upgrade Thornton's has seen marked improvements across the core areas of its business operation and in the administration and support of the remote access infrastructure.

INCREASED PRODUCTIVITY

From a business perspective the Microsoft IAG/Swivel technology has contributed significantly to the company's productivity, enabling the firm's fee earners to work more flexibly; reducing the need for non-productive journeys travelling between home and office and increasing the number of potential billable hours available each day.

INCREASED SECURITY & COMPLIANCE

The Microsoft IAG/Swivel technology is highly granular and self-managing enabling Thornton's to put in place improved security policies designed to control access to confidential files; monitor and track all network activity and ensure that devices connecting to the network have the correct antimalware software installed to prevent the spread of viruses across the entire network. Swivel, two-factor authentication ensures that Thornton's IT systems are compliant with the latest security legislation.
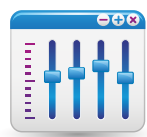
IMPROVED SYSTEM MANAGEMENT

The new system means that all someone needs is access to the internet and a Swivel PIN in order to logon, removing the need for intervention by the IT team and massively reducing the number of help desks requests- freeing up IT support time for routine network management tasks.

Since the Swivel system is tokenless it also means there are no key fobs to manage and user provisioning can be easily controlled via a browser interface removing the worry about lost or stolen fobs and deleting users as soon as they have left the company.