Making security add up

By Sonia Blizzard

Accountants are used to dealing with complex sets of data and recognise the sensitivity of the information they hold on behalf of clients. As with other professions, technology is presenting challenges which require careful consideration by accountancy firms.

In this article, internet security expert and MD of Beaming, Sonia Blizzard, talks through a few of the ways you can make sure you can make your security add up.

Security vs Flexibility

The first of these is security versus flexibility. Most accountants like to have the ability to access their systems from clients' sites or working from home, as this is efficient for their company, and they want to achieve this safely.

Remote working solutions such as Terminal Services or Citrix and hosted software platforms achieve this, as long as the company knows the servers are based in a secure location in the UK and if in a shared data centre, that this data centre complies with the highest security standards.

Ultimately the accountancy firm is responsible for the data they hold on their client and it is their duty to know where it is held and that it is safe. Under no circumstances, do they want to become the weakest link in the chain of their client's defence against online criminal activity.

Added to this there is the more basic issue of connectivity. In our experience, firms often look at the speed at the server location but forget about the experience at their office location, if different. It is pointless investing in technology if you cannot access it.

A broadband connection aimed at the residential market is not going to deliver an efficient way of working and what happens to the office if there is a fault when it takes days, rather than hours, to fix? What would happen if this was towards the end of January when last minute tax returns are being filed? In the same way that accountants are highly familiar with the regular software upgrades which need to take place for accountancy software, partners should routinely review their systems and connectivity to ensure that they have the correct network in place.

Protecting against threats on each site

For larger firms, with a number of locations, there may be a range of solutions to consider and when doing so, with the recent increase in cyber hacking in mind, security should be paramount. Each site should be protected against such threats and this can soon add up in terms of cost of hardware, but how about a private network where there is only one route in and out to the public internet?

This saves on the cost of equipment and it can also consolidate any historically different ways of working at each site to those under one arrangement, which will bring huge benefits when it comes to managing staff.

Changing attitudes towards data security

The second challenge is managing clients' attitude to data security and technology. In our experience, accountants are, on one hand, dealing with clients who have suffered from online fraud or system failures, and on the other, those who are nervous about the security of their financial information but do not know what is best practice. They turn to their trusted professional, their accountant, for advice. Those accountancy firms who have invested in their own solution to this problem and who are confident about the advice they can give will have the advantage. Imagine as well if a firm was to be compromised or to lose its systems for days. What would happen to its client base?

Accountancy firms work alongside external parties, such as bookkeepers. The trusted relationship between accountant and bookkeeper should also include an evaluation of how seriously each party takes security of the shared client's data.

Data storage and back up

Another challenge that faces accountants is data storage and backup. By the very nature of what they do, accountants hold large amounts of historic paperwork, all safely under lock and key. For those who have moved to a paperless solution, this still needs to be safe. Data backup is then the solution.

Offsite backup is essential. This is an easy piece of advice which accountants can also give to their clients. It does not require them to become IT experts or have a forensic understanding of how the client runs their systems. With the right kind of offsite backup, such as Beaming's DataChest which holds seven copies at a time in an encrypted form, if the client is compromised by ransomware such as Cryptolocker or loses their key financial information due to a system problem, the backup files will not be overwritten and they will be able to restore the files and ultimately continue to trade. That's good for them and good for the accountant.

About the Author

Sonia Blizzard is the Managing Director of Beaming – a company that provides secure internet connectivity and data back-up services to a number of businesses across the UK. Coming from a corporate background in the telecoms industry, Sonia worked for a firm which is now known as BT Global Services, setting up Beaming in 2004. The company bridges the gap between actual business needs and IT; specifically the broadband and telephone connectivity that's vital for running a business day to day.

Co-ordinates

E-mail: sonia@beaming.biz
Website: www.beaming.biz
Tel: 44 (0)1424 462661