



Don't overlook employee security screening

More and more businesses are beginning to demand that IT support staff have been vetted before allowing them access to their systems

Whether or not your company sells IT security solutions, the chances are your customers consider network security an essential part of their business. Every year, companies spend hundreds of thousands of pounds to ensure their data is kept secure, often purchasing the very latest technology in an effort to stay one step ahead of the next big threat.

But what happens next? One of your IT support technicians turns up on-site and needs unhindered access to your customer's network. Or at least he says he does. Although there are ways to limit access to sensitive data, many companies either don't know how to do this effectively, or don't bother, which means your support staff will have unrestricted access to more or less all of the information on the customer's network. For obvious reasons, this makes no sense at all.

As an industry, we have made such great strides in terms of the technology that supports data security, and yet many companies forget that the human element of all this security still represents a critical piece of the puzzle. For this reason, it is essential to ensure all your employees — especially those

who have access to customer data — have been vetted to a recognised industry standard, ie, BS7858:2006.

BS 7858:2006 is the revised British Standards Institute code of practice for security screening of personnel and individuals employed within a secure environment. This standard can be achieved by implementing NQA3000, the only UKAS Product Certification of BS7858:2006 for personnel vetting. This revised standard includes current address verification, credit check, county court judgement, insolvency, bankruptcy search, five-year written employment verification, criminal record check (CRB), and personal references. By implementing NQA3000 (BS 7858:2006) your company can prove it is adhering to industry best practice processes, while also enhancing its corporate governance and regulatory compliance requirements.

If all of this sounds terribly boring and you don't really have much interest in staff vetting, then consider this: your customers will. More and more businesses are beginning to expect — and to demand — that all of your support staff have been vetted to these standards before allowing them

access to their systems, and perhaps even onto their premises at all.

Recent research showed that 50 per cent of all CVs submitted by males in their early 20s featured misleading information, and nearly 70 per cent of job applicants had asked a friend to act as a referee on their CV. Worse still, the IT industry is home to some of the worst culprits of all. Although 56 per cent of the applications over the course of the year were found to contain lies or omissions, this figure rose to 70 per cent for IT contractors.

You've no doubt heard it said before: your employees are your

If you don't really have much interest in staff vetting, consider this: your customers will

company's biggest asset. However, at the same time, dishonest staff can very quickly bring about the collapse of an otherwise successful business. Don't let it be yours. ■

Brian Fenwick is director at staffvetting.com