Information Security Now - 3

John Mitchell

I saw a little device advertised the other day with the tag line that it 'allows you to monitor what your kids, employees, or anyone using your computer is doing while on the Internet and you can monitor them live, in real time, from anywhere in the world'. The software resides on a USB device, but once loaded onto the target machine you remove the USB host and therefore leave no visible trace of the Trojan you had inserted. No technical knowledge required and not a bad investment at £30 to enable you to subvert a machine or two. The icing on the cake is that you get two-way communication which allows you to block the target machine's internet access from any other machine with an internet connection. So spy ware and denial of service, all in one easy to use device sold openly and legitimately. Well, maybe not so legitimately in the UK. The new UK fraud Act has a clause which covers 'possessing making & supplying articles for use in fraud'. This is a catch all clause to cover the use of technologies not in existence when the Act was conceived. The problem with this is that even data analytical tools used by computer auditors could, in theory, fit into this definition. As indeed, could the search engines. It's not all bad news however, as the intent is the deciding factor. Data analytical tools and search engines were not intended to be used for fraudulent purposes. The fact that they can be used in such a way is down to the intent of the user and not the design of the tool itself. So although this little device could be used for computer crime and it does fit neatly into the unauthorized access and unauthorized modification clauses of the UK's Computer Misuse Act, it is the use to which it is put that counts. It is advertised as a way to keep your eye on what your children are up to and allows you to block access to undesirable web sites. Very laudable, but somewhat less charitable is the phrase that refers to snooping on your employees too.

Which brings me to the vexed subject of employee vetting. Vetting goes far beyond simply asking for references and copies of their exam certificates. It is more of an in-depth examination into the probity of key individuals. Some IT staff have pretty much unhindered access to a company's secrets and they are also in a position to do material damage to the company's data and software. It makes sense then, for the company to treat these peoples employment and subsequent monitoring with a little more diligence than the average clerk. However, in many cases these people are contract, or even temporary employees where the company is relying on a third-party to vouch for their integrity. What due diligence has been undertaken? I have long argued that security is primarily an HR issue, but I have received little welcome from HR when I have asked questions regarding the vetting of key IT staff. The situation becomes more complicated where a service has been outsourced. What checks is the service company doing on its staff? Can we rely on a SAS 70 statement[1] for this. Well, it depends on what is included in the SAS 70. None

[1] The American Institute of Certified Public Accountants developed the Statement on Auditing Standards (SAS) No. 70. Organizations that successfully complete a SAS 70 audit have been through an in-depth audit of their control activities, including controls over IT and related processes. SAS 70 allows a company to provide a third-party certification of its internal controls to customers.

of the SAS 70 statements that I have reviewed have explicitly covered staff recruitment, but there is no reason why you should not ask for this to be included.

John is editor of BCS IRMA's award winning *Journal* and Managing Director of LHS Business Control, a corporate governance consultancy that he founded in 1988. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or +44 (0)1707 851454.