Information Security Now - 4

John Mitchell

Information Privacy has taken several knocks recently: Nationwide building society lost the account details of eleven million of its customers; TJMAX had a similar problem with its customer credit card data and in what could be the largest data security breach to date, MasterCard International admitted that information on more than 40 million credit cards may have been stolen. The methods used by the perpetrators may have been different in each case, but the end result is the same. The customers concerned are severely inconvenienced and with the threat of identity theft hanging over them for years to come. In the case of Nationwide the FSA imposed a record fine, but the Information Commissioner's (IC) office did nothing, despite being responsible for overseeing data protection. Their rationale being that as the FSA had already fined Nationwide it would be churlish to hit then twice, especially as the customers ended up paying the fine as it is a mutual society. While not disputing that aspect I would have thought that the IC should have a least insisted on the company disclosing to each of its customers details of their data that had been stolen and to pay for annual credit checks for the next few years. No so. Nationwide hid behind "security" and the IC took this lame excuse at face value. So the criminals may know Nationwide's customer data, but the poor customers, who have ended up paying the FSA fine, have no idea what data of theirs has been stolen. If that is not a perverse situation, then I don't know what is.

Most organisations have secure primary systems, but security falls apart when the data is removed from the secure system and put into the end user computing environment. This occurred at an NHS Primary Care Trust where patient data was downloaded from the secure patient record system to a local workstation hard drive and was then transferred from onto a PDA. The PDA was then lost on the public transport system. These actions clearly breached the Trust's security policy, but as the person involved was a temporary employee there was little in the way of sanctions that could be applied. Security is a people, not a technical issue. I have never know a computer make a conscious decision to disclose, or steal data. We can control the technology, but only manage the people and therein lies the problem. People will always be the weakest link so we need to design our systems to detect abuse by the people. You will notice that I write "detect" and not "prevent". People will always find a way to circumnavigate security, but if they know that they will be caught it may stop them trying in the first place.

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.