Editorial

For some years I owned an Ericsson SH888 mobile telephone. It was a neat little package with a modem included so that I could link up to my laptop, surf the web and deal with my email while on the move. Not very different from any other modern mobile I hear you say, but where it really scored was with its inbuilt security. If the keyboard wasn't used for twenty seconds it automatically locked itself. When you next wanted to use the telephone you had to enter your pin code to unlock it. Far superior to the Nokia junk that has now replaced it. The poor Ericsson was dropped on its head one day and was never quite the same afterwards. It made perfect outgoing calls, but incoming was a bit suspect – a blessing for most people, but not good for my business. My point on the security aspects are that mobile telephones are becoming the de facto input and output devices for computerised applications. They will need excellent security, but it seems to me that the major manufactures are only playing lip service to this. Just think of the problems with my Nokia. First I have to manually lock the keyboard by pressing two keys. To release the lock I press the same two keys. Now if someone else gets hold of my Nokia and it is already switched on, then all they have to do is release the key pad by pressing the two keys and they can use my service free of charge. If I am connected to my email at the time of loss, then they effectively become me. I don't have the option of setting a security code. The manufacturers need to do something, but they will not do so unless pushed by their customers. So it's up to us.

I am the Group's representative on the BCS's Security Expert Panel (SEP) and one of the tasks I recently picked up was to evaluate the syllabus of the European Computer Driving Licence (ECDL). An oddly names qualification, but one that has a lot to offer as is shown by the fact that over a million people have seen fit to take the examinations that lead to the award of the qualification. Basically it shows that the holder can find their way around the major office applications in everyday use: such as word processing, spreadsheets, databases; email, presentations and the internet. They are also required to show that they understand the basics of the operating system, including the security aspects, which are dealt with in the first part of the syllabus. Despite its strange name this is a very useful qualification as it shows that the holder really does know how to use a computer and is aware of the need for security. It's not a 'Noddy' qualification either as it requires 150 hours of study and the passing of seven examinations. Full details can be found at www.ecdl.co.uk.

Remaining on the security theme, the main article in this edition is the report by the Electoral Commission on the security aspects of the recent electronic voting pilots in the May local elections. The article is based on the Commission's overall conclusions from the 17 pilots. All the individual reports and the full text of the summary can be found at www.electoralcommission.gov.uk and they make interesting reading. We should all take an interest in electronic democracy. The whole idea of pilots is to learn from them and I hope that the Government does so.