A question of perception

Stuart Notholt FCIJ reviews Information Security for Journalists, by Silkie Carlo and Arjen Kamphuis, Centre for Investigative Journalism (http://www.tcij.org/resources/handbooks/infosec).

Whether the emergency information surveillance laws recently rushed through Parliament are a 'snoopers charter' or, to quote the Prime Minister, a vital tool to "keep the country safe" depends not just on an assessment of terrorist and criminal threats, but how cynical one is about the honesty and intentions of the government. Similarly, whether you see Julian Assauge or Edward Snowdon as heroes, traitors, or simply self-publicising fantasists will derive largely from how credible you regard their allegations. For most people the issue will boil down to whether they trust and believe the 'whistleblowers' more than the government spokesmen who claim that surveillance is carried out within a strictly regulated legal framework.

The authors of Information Security for Journalists are in no doubt as to where they sit on this continuum. Their booklet is dedicated to the 'whistleblowers', and the claims made by Edward Snowdon in particular are accepted uncritically. To Carlo and Kamphuis, governments are active participants in the suppression of journalists as they perform their key function, which, in quoting William Randolph Hearst, they see as "writing down what powerful people and institutions do not want written". They note that the Mexican army spent $350 million on surveillance tools between 2011-12, and that nine Mexican journalists were killed in work-related incidents during the same period. The inference is obvious.

That said, the main external threats to the vast majority of UK computer users still comes from 'regular' cybercrime or the physical theft of equipment (and thus the data stored on it). Even if British government scrutiny is as intrusive and all-pervasive as Carlo and Kamphuis believe, the chances of the average citizen being of serious interest to the security forces remain pretty low. Even the 'average' journalist (if there is such a thing!) would probably not be a 'person of interest' unless and until their investigations stumble across something juicy. So we need to consider which parts of the advice in Information Security for Journalists are applicable to the citizen at large (including many journalists) and which are more relevant to investigative journalists who believe they need heavyweight data protection.

For example, their guidance on encrypted folders would be of application to most citizens. It makes sense for everyone to have an encypted folder or drive in which to keep confidential data and records. Large organizations already invest in encypted email technology and, again, there may be occasions when it is useful for the individual to encrypt a particularly sensitive piece of correspondence. Where they urge the use of untraceable web browsing techniques, a second 'air gapped' laptop (i.e., one which never, ever, goes on-line), and a secure open source operating system the case is more ambivalent – not least because these are surely the self-same techniques that would be used by paedophiles or terrorists. Might, perversely, possession of such systems not in themselves draw undesirable attention to the user? And at the end of the day, the State can always resort to what Carlo and Kamphuis coyly call "extreme lengths" if they want to get hold of somebody's passwords.

So, how worried should we be about someone gaining unauthorized access to our valuable data? About government snooping, the answer is, candidly, we simply don't know. Concerning data

breaches in general, however, a distinctly alarming picture emerges. According to figures published by the Department for Business, Innovation & Skills last year, in 2012 63% of small businesses suffered a data attack by an unauthorized user. However, more than half (57%) were 'inside jobs' – i.e., staff-related security breaches – rather than hacking by the state or outside cybercriminals. Admittedly, the majority of these stemmed from accidental loss of data (the laptop left on the Tube syndrome) – but 10% of staff breaches were identified as being deliberate and malicious. In other words - and ironically Snowdon rather proves this point - the biggest risk to your organization's data doesn't come from criminals or governments: the 'motivated intruder' is just as likely to be on the payroll.