The IT Detective

Just like Sherlock Holmes, computer audit consultant John Mitchell's methods are elementary he asks the right questions. Alison Classe gets on his trail and discovers the job is filled with challenge and variety

For computer audit consultant John Mitchell there's no such thing as a routine day. After checking his diary before turning in last night, he knows today's first appointment is an easy drive from his base in Potters Bar. He's due at a meeting with a large public-sector client which recently called him in for some detective work on a live system. Having discovered corrupt record linkages on the database, the client suspected sabotage. Like Sherlock Holmes, Mitchell insists his methods are elementary. 'A lot of my time is spent not doing any-thing fancy or technical, but just talking to people, in a simple but structured manner. 'First, I ask what's happened over the past few weeks to change the system. Often they'll say: "Oh, we released a new version of the program," or "we got in a new member of staff. " Usually the problem boils down to something having changed. 'In this case, after interviewing all concerned, Mitchell has ruled out sabotage and has reconstructed the chapter of accidents leading to the corruption of the pointers. 'Most breaches of security are accounted for by a lot of small things going wrong together, rather than one large thing on its own. Here, the firm had implemented new database management software and it hadn't been clear from the documentation that it ought to have restructured the database. A contributory factor was that the technical support person was on holiday and his stand-in was sick, so the change had been implemented by a third, unqualified person. 'The reason they continued processing regardless of the errors, was that, although they normally ran a nightly check on database integrity, they hadn't had time because another system was going in,' he says. Today, Mitchell is presenting his verdict to the management, a task he anticipates with mixed feelings.

'There are three possible reactions to my diagnosis. One is to say: "That's so simple we could have found it out ourselves you're a waste of money. "'The second is for senior managers to kick someone. Sometimes a manager will say: "I want you to name names!" My reply is always: "lf l put a name in this report it will have to be yours. " We're always trying to educate management to accept that control is its responsibility. 'The third reaction is rarer management decides to implement a proper control structure. ' This reaction, of course, is the one Mitchell is keen to promote. 'We prefer to do preventative work ideally before the system goes in. ' But not being called in until the problems start is fairly typical, he adds ruefully. This morning, after presenting his explanation of the database problem, he spends some time discussing possible control improvements with the managers. Selling control can be an uphill struggle. 'Control isn't sexy. What's more, management always thinks it's being done anyway. My opening move is to ask: "You've been talking about controls; now how do you define them?" At that point they go slightly incoherent, so I get in with my definition: a control is anything which monitors or modifies the behaviour of a system so as to make it predictable. That predictability is something management craves but doesn't know how to go about attaining'. Managers are wary of being sold yet another methodology. But Mitchell warns: 'The development methodologies pay lip-service to control. Some only devote a line or two to saying what you have to do. 'Another problem is quantifying the value of audit work. I once found a mistake in the major calculation of a system which was about to be installed at 250 sites. All I did was run a few tests which should have been run anyway. The test team had taken the results as being near enough. Correcting the mistake at 250 sites would certainly have been expensive, but it's hard to say how expensive. 'Ironically, computer fraud, the one bugbear that makes management sit up and take notice is rare. I've come across three frauds in 15 years. Two were input frauds: somebody changing a docket before it went into the system. The third was more sophisticated.

It was a financial controller who used to prepare all his monthly returns on a spreadsheet and send them in to head office, balancing beautifully and printed neatly on a laser printer. Because he was always meeting his targets and none of his colleagues were getting anywhere near, management eventually became concerned about the accuracy of his spreadsheets it didn't suspect anything more. When I went along to get copies of the spreadsheets this person became very obstructive. That always rings alarm bells. In the end, I had to go at the weekend, with a key given to me by one of the directors, to take the copies off his machine. It took a while to track down what was going on. The clue was the spreadsheet files had a time and date stamp, and I noticed some had been updated as late as 11pm. I knew from the clocking in records he shouldn't have been there at that time. And why change the files so late at night? 'What he'd been doing was putting any figures he liked into the spreadsheet to give the required rate of return. He didn't stand to gain any money out of the system, although he was on a performance related bonus for meeting his targets. But I think it was mainly a matter of pride'. Three frauds in 15 years isn't A lot. Mitchell says: 'I've no doubt much more money is lost through mistakes than through fraud. But if you have loopholes in your system that can lead to accidents; those loopholes can equally well be exploited by

someone who wants to subvert the sys tem. Good controls guard against both'. Unsure whether his sales pitch has worked on this morning's customer, Mitchell departs for a working lunch in London with the chairman of the London Chapter of the Electronic Data Processing Auditors Association[1], a sister group to the BCS Computer Audit Specialist Group[2], which Mitchell himself chairs. The two compare their respective groups' schedules for the coming year to check there are no clashes on dates or topics. In the afternoon, it's off to another client, a large commercial concern south of London. This time Mitchell's brief has been to review a system specification to ensure adequate controls are built in before coding starts. An assignment such as this indicates that the 'prevention not detection' message is getting through, at least in some quarters. At the meeting, Mitchell discusses the spec with development staff and users. His constructive suggestions for additional controls and other safety measures are accepted and will be incorporated into the design. Mitchell goes on to remind his customers that their controls will need overhauling regularly. 'Here I invoke the second law of thermodynamics: any ordered state becomes disordered over time. A company will start off, per haps having had a bit of a scare, and put in a nice control structure. Then it will carry on, regardless of changes, until something else goes wrong, prompting comments such as: "Hey, but we've got a control structure this expensive consultant recommended two years ago." However, because of entropy the structure's no longer valid. 'This particular system is being implemented on a minicomputer, but with the increasing popularity of PCs and PC networks, viruses and software piracy are becoming major issues for auditors. Mitchell claims that, thanks to the Federation Against Software Theft and its dawn raids on suspected software pirates, as well as virus scares, most large firms are now aware of their responsibilities and are implementing inventory and other systems to ensure all software is legitimate. But in smaller companies this conscientiousness is by no means guaranteed. Mitchell cites one internal audit department whose head justifies illegal software copying on the grounds that the company cannot afford to buy the packages. Generally, Mitchell encounters a gamut of attitudes to software loading. 'At one extreme, there are places that have no rules at all and, at the other end, there are those where it's a sackable offence to load a diskette that hasn't been through the correct channels. 'Some companies have software-based methods to control what can and cannot be loaded: for instance, software that scans for viruses or applies a checksum technique to see if code has been modified. But to have those checks on all your machines can be counter-productive if you need to load new programs often. Some people have tried this type of protection and found it not worth the effort'.

Mitchell is sometimes called in to assess the extent of piracy. This task involves both physical checking of the , company's PC disks and chatting to users. It can be tricky to spot a situation where there are 10 licences and 15 installed copies just by looking at PC disks. 'The best way to find out if a piece of software is legal is to ask the user of the machine for the master disks. 'If those are lost, then I ask for the manual. If they can't provide either the disks or the manual, then nine times out of 10 it's an illegal piece of software. Again,

[1] Now the International Audit & Control Association (ISACA)
[2] Now the Information Risk Management and Audit (IRMA) specialist group

it's just a matter of asking the right questions'. Mitchell doesn't expect a warm welcome when he's acting in what he calls his policeman capacity. But some people will tell him things they wouldn't tell their own managers. 'Audit often has a reputation for getting things done. Because audit reports go to very senior people, the person at the bottom of the heap sees an opportunity to get something communicated to the top. You have to be careful about verifying what you're told'. Unlike a real policeman, Mitchell isn't interested in motives. 'I look only at facts. You'd go mad if you started thinking about personalities. You'd wonder why, for instance, a guy in charge of a departmental budget of £1 million needed to use pirated software'. Alongside prevention and detection, education is the third main area of Mitchell's work. On the way home, he drops in at a training company for whom he's due to give a course on PC security. Then it's back on the M25 for the trip home. Mitchell, who trades under the banner of LHS Business Control, works with four associates, all computer auditors. This evening they're combining business with pleasure and doing their 'associating' in the pub.

Reproduced from *Computing* – 30 July 1992