Information Technology and the management of corruption

Richard Heeks

Introduction

Corruption — 'inducement to wrong by bribery or other unlawful or improper means' — is a global problem and one that tends to stir strong reactions (adapted from Klitgaard 1984):

- corruption is a culture-bound concept: 'Your culture may say that X is corrupt; mine does not';
- corruption is a force for good: 'It helps the wheels of government and business to turn';
- corruption is too big to deal with: 'Corruption is everywhere. What can we ever hope to do about it?'.

All of these reactions can make it hard for corruption to be addressed by development managers. Yet it is an issue that many of them face, and which must be attacked for at least three good reasons (adapted from Davies 1987):

- it drains off valuable economic resources, particularly investment funds, into unproductive uses, and reduces the likelihood of development objectives being achieved;
- it siphons off another valuable resource — the time of development organisation staff — into unproductive use, and creates resentments and frustrations among staff, thus reducing organisational efficiency;
- because it is hidden and unaccountable, corruption is essentially undemocratic and hampers the development of democratic processes and institutions.

One currently-dominant paradigm of corruption control — termed the 'Panoptic vision' by Anechiarico and Jacobs (1994) — sees management techniques of rules and enforcement as the key to controlling corruption. Enforcement is, and has always been, a labour-intensive and information-intensive activity for which managers require assistance (Sparrow 1992). One model for such assistance is provided by Jeremy Bentham's nineteenth-century idea of the Panopticon: a constructed technology that allowed a single central unseen guard to observe the activity of all prison inmates. In the late twentieth century, information technology (IT) presents organisations with the possibility of creating their own Panopticon: one that would allow managers to gaze unseen upon the activities of their employees and thus monitor and control corruption (Roszak 1994; Ramasoota 1998).

But what of reality in development organisations: can information technology, in practice, help control corruption? Some thumbnail sketches are offered below to help provide initial pointers to an answer. The cases are drawn from the experiences of the author and of development managers studying at the University of Manchester.

Cases of IT and corruption

Case 1

Managers in a railway system were concerned about the efficiency of its seat and berth reservation system, and about corruption within the system. Booking staff had access to, and control over, the allocation of places on trains. A few would take a bribe (either directly or via a ticket tout) to provide a passenger with a reserved place; these being at a premium since all trains were over-booked. A computerised system was introduced, one objective of which was to eliminate corruption. To achieve this, allocation of reservations was handled automatically, including the particularly 'weak link' of moving passengers on the waiting list into places vacated by cancellations. Computerisation did make it harder for the clerical staff to be corrupt because the software, not the clerk, now decided — based on booking date — which passengers would fill vacated slots. However, corruption was not eliminated, and two aspects will be noted here.

First, station managers retained manual control over a certain proportion of the train places, supposedly to cover emergencies or last-minute travel by VIPs. Some continued to provide these places to non-

emergency, non-VIP passengers in return for cash. Second, ticket touts showed how ingenious and resourceful they can be. Knowing that their best customers were businessmen in a hurry, they would book places well in advance on the main inter-city trains using a very common man's name, citing his age as 35 years. These places would then be sold at a premium to last-minute travellers, most of whom were men who could get away with appearing 35 years old to the ticket collectors.

Case 2

In a public works department, there was concern about the number of 'ghost workers' in the system. These are people listed on the payroll, and therefore paid, who do not exist in reality. Someone else collects the wages paid out under their names. The payroll system was computerised and, during this process, a check was made between listed and actual workers. Any non-existent staff were removed from the system.

This seemed to have solved the problem, assisted by the word being spread that the computer could make an automatic check between the payroll list and reality, and could automatically detect who was picking up ghost worker wages. Of course, it could do no such thing. An audit 18 months later uncovered a very well-to-do computer operator who was collecting his own wages plus those of 30 other workers he had entered into the payroll system.

Case 3

Examination marks at a university were previously kept on paper, with calculation of final grades and averages being done manually by a small group of trusted staff. Mark lists were kept locked in a safe when not being used. Given the large number of students, it was decided to computerise the marks and calculations. There was an assumption that information on the (un-networked) computer would be safe, though a password was added just in case, known only to a very few staff.

All seemed well until one lecturer noticed that a low-achieving student had obtained a spectacular final grade. Enquiries revealed that he was the son of one of the computer managers. The manager, knowing the importance of university grades for job prospects, had opened up the marks database and changed his son's mark. Unfortunately for him, instead of altering the figures slightly, he was over-ambitious and pushed them from the 40s up to the 70s.

Case 4

Computerisation was taking place in a (different) university, and it seemed obvious to turn attention to the admissions process, which was notoriously slow and corrupt. Computerisation of admissions involved entering the school-leaving exam marks of all applicants, and then producing a prioritised list, headed by the candidate with the best overall marks. Other factors might be taken into account but, if all other things were equal and there were 1,000 places at the university, the top 1,000 candidates on the computer-generated list would be the ones to gain admission.

This clearly represented a considerable threat to members of the admissions committee. These members could gain significant financial and political rewards by offering places to children of the rich and powerful who would not get into university if an entirely merit-based system were adopted. The committee therefore decided to accept the prioritised list merely as an 'advisory tool', and never made it public outside that committee.

Case 5

A customs department kept manual records with the names and addresses of overseas firms which had been involved in import or export transactions. These contacts were useful to local entrepreneurs, particularly those seeking export collaborations. The entrepreneurs therefore paid customs officials to provide them, illegally, with the contact details. The department, including its overseas firm details, was computerised and one computer was put into a front office where members of the public could access it. Entrepreneurs gained direct access to the contact details they wanted and payments were therefore no longer made.

Information about foreign businesses was a resource which local businesses required. Because the information was scarce and because it was kept as a private resource, customs officials (acting as information 'gatekeepers') were able to charge 'rent' for access to it. Once the information came into the public domain, no access charges could be made.

Impacts associated with introducing IT

From these cases, we can conclude that the impacts associated with the introduction of IT are quite varied:

Removal or detection of some corruption

Corruption in an organisation is possible because staff have access to a valued resource and to those who will pay for it. The valued resource could include provision of a service, legal permission to undertake some activity, or information of value. They also have the skills, confidence, and autonomy to make decisions about the provision of that resource.

Where IT can deny access to the resource or to relevant decision-making processes, this may remove corruption. Typically, this will occur if the processes are automated. For example, the clerical staff in Case 1 no longer had control over allocation of vacated reservations. In other cases, computerisation assists detection of corrupt practice, in line with the Panoptic vision. In turn, this reduces staff's perceived autonomy and so is likely to suppress some corrupt practices.

New corruption opportunities

In Cases 2 and 3, the introduction of IT provided new corruption opportunities for some staff. This phenomenon may often be related to closing down opportunities for other staff. Computerisation does so by creating changes in one or more of four aspects:

- *Skills*: computerisation is often associated with an 'up-skilling' of corruption, providing an opportunity for those with IT skills, and denying those without these skills.
- *Confidence*: borrowing from the Panoptic vision, a mythical image may be promoted of the computer as an objective, all-seeing, all-knowing machine. This may cause some corrupt staff to lose confidence and to refrain from corrupt practices. Those who understand computers are not put off (and will often spread the myth in order to reduce the likelihood of competition or detection).
- *Access*: in the cases described, computerisation of records was accompanied by closing down access to some staff but opening up access to all those operating the IT systems. With the advent of networked systems, such opportunities for access may greatly increase.
- *Control*: the mask of data quality and computer omnipotence makes some managers assume that IT removes the opportunities for corruption, i.e. that the Panopticon can operate without the need for human intervention. They may therefore fail to institute controls on computerised systems. This assumption provides greater autonomy for IT-literate staff.

No effect on corruption

In Case 4, and for the station managers in Case 1, computerisation had no effect on corruption. This is because computerised information systems were designed in such a way that key corruption-linked resources or processes were left uncomputerised, despite their possibly being surrounded by other computerised systems.

Factors determining the impacts of corruption

These different impacts can be explained by the different factors involved:

Information technology

Computers have no innate property related to corruption except that of their imagery. They do not automatically provide a Panoptic model of control — this only comes if they are deliberately and systemically designed to do so. The impacts described above, therefore, principally depend on the design of information systems and of wider organisational systems.

Information system design and management decisions

The way that computerised information systems are designed significantly determines the impacts of corruption. This design, in turn, depends on management design decisions. In Case 1, for example, it was a management decision that led to automation of clerical procedures and, therefore, to the removal of one opportunity for corruption. On the other hand, a management decision was taken to avoid computerising the station managers' allocation of emergency and VIP places.

To some extent, this latter design decision was part of the process of getting computerisation accepted: it was only able to proceed once the decision had been made that computerisation would not threaten these stakeholders' control and private incomes. Indeed, by removing sources of competition for corrupt earnings from the clerical staff, computerisation potentially offered an opportunity for station managers' incomes to be increased.

Other information system components will also affect the impacts of corruption. For example, the design of work processes will play a role. In Case 5, the presence of IT is largely irrelevant: the department could have made its manual records publicly accessible, which would have led to a

similar result. What mattered was a management decision about the wider re-design of processes that changed the way information flowed in the organisation. Similarly, in Case 2, computerisation had little to do with the removal of ghost workers or claimants and the consequent (temporary) removal of corruption. This required the introduction of a process of physical checks, as was done both before and after computerisation.

Thus, it is management decisions about the design of an information system that shape the ultimate impacts. These decisions and designs do not always adhere to the Panoptic vision, with the consequent implications for corruption control.

Finally, there are other, wider systems components that play a role. For instance, the people involved must have some motivation to act corruptly. In part, this depends on fear of detection (which computers may affect), but in the main motivation relates to the wider context, as discussed below. Managers, and others charged with guarding against corruption, must also themselves have the skills, motivation, authority, and means to detect and act against corrupt activities. In part, this too depends on wider structures, strategies, and culture.

Organisational and environmental factors

Leaving aside the 'corruption of opportunity', such as that which arose in the payroll case, two particular types of corruption can be distinguished. 'Corruption of necessity' is practised by poorly-paid, low-level staff. Their incomes do not meet the many demands placed upon them, and they must find ways to supplement them. Computerised information systems may be designed to suppress some of their activities. However, these new systems will not extinguish the underlying motivation for additional income, because this arises from a wider context. Thus, corruption is almost bound to re-emerge, as it did with the ticket touts in Case 1. The Panoptic vision is a poor guide to this reality because IT cannot (yet) monitor all activities of all staff.

Alternatively, there is the 'corruption of greed' practised by senior staff. They have enough income to live on, but want and get more, because they are in a position to do so, and because it is seen as a natural activity for those in power. Given the power of these staff to determine their working environment, computerised information systems are unlikely to be allowed to have much impact unless imposed by a very strong external agency. Such staff will, therefore, remain aloof from any Panoptic gaze, exposing a further limitation of the vision as a guide to action.

In all cases, it can be seen that corruption arises from a combination of two sets of factors: the micro-level (the individual, his/her circumstances, needs, skills, access, confidence, and autonomy) and the macro-level (organisational and national management systems, politics, and culture). As we have seen, management decisions about computerised information systems may affect skills, access, confidence, and autonomy. However, they are most unlikely to affect the personal or environmental drivers behind corruption. Hence, the Panoptic ideal of corruption controlled by IT is, therefore, flawed.

To put this in simplified terms, IT-based systems guided by the Panoptic vision affect symptoms of a corrupt system rather than causes. Corruption is a phenomenon rooted in the cultural, political, and economic circumstances of those involved. IT does little to affect these root causes, remains limited in its surveillance potential, and so cannot eliminate corruption.

Development managers require a more holistic vision of corruption control to supersede the Panoptic vision. This would understand the roots of corruption, not just the symptoms. It would address corruption not through individual management techniques, but through strategies of institutional and contextual development. It would also see IT as having a potential role, but one which is limited and which forms only one small part of a much larger jigsaw.

Managing the introduction of IT in corrupt environments

Despite the preceding analysis of IT limitations, experience suggests development organisation staff often perceive that introducing IT is going to have a significant effect of reducing corruption. These perceptions will feed into the process of planning any new information system. The effect of these perceptions is likely to be particularly marked where a new computer system is being introduced in the presence of practices that are currently corrupt.

In one government's pensions office, for example, computerisation was roundly resisted. Many factors were at first seen to underlie the resistance including:

- fears of loss of jobs;
- fears that staff would not have the necessary skills;
- health and safety concerns.

What emerged during investigation, however, was that the main fear lay around the issue of corrupt incomes. Pensions staff had the power to deny claimants access to pension payments or to provide claimants with access to certain types of higher-income pension. The staff were using this power to extract bribes from pensionable claimants. They feared that computerisation would remove this power; hence their true reason for resistance.

Where resistance and corruption are linked in this way, there are three possible reactions that can be drawn from the case-studies above:

- if the computerised system will not have an effect, make this (subtly) clear;
- if the computerised system will affect corruption and the stakeholders are not that powerful, then 'tough it out', i.e. push on in the likelihood that resistance can be overcome;
- if the computerised system will affect corruption and the stakeholders are powerful, change the design plans so that the key corrupt processes are not computerised or are not exposed to monitoring by IT.

'Toughing it out' can also be tried in the last case, and this would seem to be the morally-correct route to take. However, it will greatly increase resistance to IT and the risks of information system failure.

Whatever the reaction, it is clear that the link between IT and corruption will have to be recognised in the planning of some information systems. This link must also be teased out as a component of resistance to computerisation.

References

Anechiarico, F. and J. B. Jacobs (1994) 'Visions of corruption control and the evolution of American public administration', *Public Administration Review* 54(5): 465–73.

Davies, C. J. (1987) 'Controlling administrative corruption', *Planning and Administration* 2: 62–66.

Klitgaard, R. (1984) 'Managing the fight against corruption: a case study', *Public Administration and Development* 4: 77–98.

Ramasoota, P. (1998) 'Information technology and bureaucratic surveillance', *Information Technology for Development* 8(1): 51–64.

Roszak, T. (1994) *The Cult of Information*, Los Angeles: University of California Press.

Sparrow, M. K. (1992) 'Informing enforcement', *Informatisation and the Public Sector* 2(3): 197–212.