Suitable case for treatment

Insufficient testing is the bane of many a promising IT project, but in most cases it leads to nothing more than frustration on the part of the end-user.

In healthcare IT the need for testing is much more important in that there can be serious consequences for patients if systems are not working properly. But there is very little regulation of products and services, or of their suppliers.

This contrasts with the regulations governing drugs companies, where more than half the typical 12-year development time for a product is likely to be spent on safety and efficacy studies before the Medicines and Healthcare Products Regulatory Agency lets it go to market.

The argument that IT systems are largely administrative and therefore do not require a similarly rigorous level of scrutiny does not hold water. In hospitals and surgeries, administration and patient care cannot be so easily separated. As Tony Collins points out on page 8, delays to hospital appointments, for example, because of IT problems can cause emotional distress to patients and have potentially serious clinical implications.

Naturally everybody involved in developing systems wants to deliver benefits at the earliest possible moment. But every IT user, whether in healthcare or in business, knows that most systems when first delivered contain faults which need fixing before the system does what has been promised.

This danger of buggy systems can only be pre-empted by rigorous testing and remedial action before delivery, even it means delays. Patients, unlike business executives, do not have the luxury of withholding payment until problems are fixed. They need the protection that can only come by an appropriate level of regulation of healthcare IT systems and services and of their suppliers.

 Computer Weekly 16/1/07

User testing is strengthened after project runs into trouble

Passport agency goes public on test errors

Tony Collins
tony.collins@rbi.co.uk

The Identity and Passport Service is strengthening its testing programme for IT projects after an investigation into the failure of a project to process passport applications online found that insufficient testing and checks were partly to blame.

And in response to Computer Weekly's campaign for greater openness, the government agency has published a report on the lessons it has learned from this and its other key IT projects in 2006.

Bernard Herdan, executive director of service delivery, said the agency had changed its approach to testing on IT projects in the light of the internal inquiry's findings. And he challenged other central departments to follow suit by publishing lessons learned from specific projects.

After the problems it encountered last year, the agency is doubling the time allowed for user acceptance tests, from nine weeks to 18 weeks, on its latest project. The scheme involves building systems that will support agency staff when they help authenticate passport applications by personal interviews with applicants.

The change of approach comes after the agency's inquiry into the failure last year of its Electronic Passport Application system, known as EPA2. The inquiry found that too much work had been left to the agency's main IT supplier, Siemens Business Systems.

When EPA2 went live in May, passport applications became jammed in the system, there were "quirks in the software", and performance slowed to the point where a backlog of 5,000 applications built up.

The report on the lessons from EPA2's problems said that, because of the supplier's strong track record, the Identity and Passport Service had "relied on Siemens Business Services for technical assessments and should have done more to ensure testing was done".

The agency added that it needed to "develop further our technical capability to challenge supplier assertions and to develop more comprehensive acceptance test plans".

Herdan told Computer Weekly that Siemens would pay for the cost of correcting EPA2. The system's design will be simplified before the software is rebuilt and brought back into service, perhaps next summer.

"The EPA2 system as delivered was considerably more complex than initially intended. In isolation, each change was assessed... but together [the changes] rendered the system too complex and much more difficult to test," said the report.

The EPA2 project team also acknowledged that they had given too low a prominence to the risks of poor performance of the system when it went live.

After the failure of EPA2 last year, Computer Weekly issued a challenge on BBC Radio 4's You and Yours, calling on the Identity and Passport Service to publish the lessons learned from the project.

But the agency decided to go a step further and publish the lessons learned from all three of its key IT projects in 2006.

"We thought it important to get the lessons out," said Herdan. "We will continue sharing our lessons at the risk of people saying, 'Fancy them getting that wrong, didn't they know?'"

Tony Collins and Bernard Herdan interviewed on BBC Radio 4
→ www.bbc.co.uk/radio4/youandyours/items/02/2006_28_tue.shtml

Read Tony Collins' blog
→ computerweekly.com/blogs/tony_collins

A step forward, p18

Open book: project lessons were published after Computer Weekly challenge

KEY POINTS

- Identity and Passport Service goes public with lessons of key IT projects
- Testing boosted after inquiry into online passport applications system
- Report says the agency relied too heavily on supplier for testing
- Director urges other departments to publish lessons learned from projects

Computer Weekly 30/1/07

Openness is key to effective project management

Hands up, who wants to avoid IT disasters?

A corporate antipathy to criticism, and a welcoming of positive comments only, or even affected optimism, can be early warning of an IT disaster

Tony Collins
Opinion

"If things go wrong with government IT we should hold our hands up, fix the problem or learn the lessons." So said Cabinet Office minister Pat McFadden this month.

Nobody could argue with this. But when things go wrong with government IT, nobody does hold up their hand and admit responsibility. Investigations of the causes of dozens of large IT-related failures show that organisations tend to react to crises in similar ways: they try to cover up.

But a corporate antipathy to criticism, and a welcoming of positive comments only, or even affected optimism, can be early warning of an IT disaster.

In private and public sectors alike, secrecy and cover-up can be part of the DNA, but it is more generally injurious in the public sector – which is a pity because hiding the specific lessons from mistakes debases the work of thousands of IT staff in the public sector who are helping to keep hundreds of complex systems running smoothly in what are often difficult circumstances.

Cover-ups continue

It takes only a small number of cover-ups over major failures to sustain the impression among MPs, taxpayers and the media that government IT and incompetence are synonymous. Yet the cover-ups continue.

Computer Weekly's requests under the Freedom of Information Act for details of particular IT projects involving the Department for Work and Pensions, the Office of Government Commerce (OGC), which oversees IT projects in central government, the Department of Health and the Cabinet Office have been rejected emphatically.

The OGC, for example, is spending tens of thousands of pounds of public money on legal fees to fight a decision by the information commissioner that the results of Gateway reviews on the progress of the ID cards project be published.

Some OGC executives would prefer to be open about mistakes made on government IT projects, but the organisation's culture, and that of Whitehall generally, requires that openness is seen as an evil spirit that visits sleepers during a nightmare.

Whitehall officials prefer to publish reports that praise everything to do with IT, though few lessons will be learned from running commentaries from the observation tower at Heathrow Airport on the safe landing of planes.

Refreshing change

So it is refreshing to note that the Identity and Passport Service is being open about the lessons and mistakes in its key IT projects (Computer Weekly, 16 January). If all organisations followed the lead of the Passport Service, it would help to dispel the mystique over IT project management.

More importantly, openness and honesty in reporting how and why projects have gone wrong would go a long way to making directors, or ministers, more accountable for failures.

While there is secrecy, they can take comfort during any IT-related failure that the full facts will probably not emerge. If they know the truth will be told, they may do more in future to avoid a costly IT disaster.

MORE ON THE BLOG

For more on the lessons learned from the Passport Office and other IT projects, read Tony Collins' blog.
→ www.computerweekly.com/blogs/tony_collins