

**Evaluation of the Department of Corrective Services  
Central Breach Unit (2006)**

**Summary Paper Prepared For:  
Australasian Evaluation Society  
Annual Conference  
Fremantle, Western Australia, September 2008**

**Dr Shona Hyde  
Senior Research and Evaluation Officer  
Strategic Planning and Review  
Strategic & Executive Services  
Department of Corrective Services**

**Introduction**

One of the biggest challenges we have as evaluators is often the uncertain reliability of statistical data. What often happens is that when you begin an evaluation you take a cursory look at the types of data that are collected and you think that you will have what you need to get a pretty accurate picture of the current state of play. Once you start downloading the data, however, and try to analyse it, you often discover so many gaps and inconsistencies that you can't even answer some basic questions such as who used a particular service or program and when. The question is: what do you do then? What do you do when the critical statistical data that you need to underpin your evaluation simply doesn't add up? And how do you ensure that the resulting evaluation still provides the type of information that is going to be useful to the key stakeholders. When your statistical data lacks credibility, what form of evaluation and what sort of methodology are most likely to provide information that is genuinely useful and could be expected to lead to tangible program improvement? More importantly, how does your role as an evaluator change to meet the needs of your key stakeholders?

In this presentation I want to talk about how I attempted to overcome the challenges posed by the lack of reliable statistical data in an evaluation of the Department of Corrective Services' Central Breach Unit. I want to talk about how my role changed, quite dramatically, as the evaluation evolved and changed shape in order to reflect the availability of data.

**The Central Breach Unit**

The Central Breach Unit, or CBU, was established in 2004 to take over the administrative tasks involved in breaching offenders that have failed to adhere to the conditions of their community based orders. Nearly 5000 people are sentenced to a community corrections order in Western Australia each year. While over half of orders are completed successfully, over 40 percent of orders are not completed on an offender's first attempt. The offender either fails to meet the conditions placed on them, e.g. by doing something like not turning up to drug testing (non-compliance breach), or they re-offend while on the order (re-offending breach). When either of these things happens, a breach action is initiated against them and they are required to return to Court.

It is the Central Breach Unit that processes this breach action, which requires the meticulous preparation of a great deal of evidence and paperwork. The case for the breach has to be proven in a Court of law in the same way that any other criminal offence has to be proven. This means that the paperwork supporting the breach case has to be completely accurate. It is incredibly important that it is done properly and that it is done quickly. The quicker you process a breach action the more likely it is that you will be able to re-engage the offender and get them to complete their order successfully, and the less likely it is that they will reoffend. At the same time, the longer it takes to process a breach action the more likely it is that a disengaged offender will have moved on and you will be unable to find them.

Prior to the establishment of the Central Breach Unit, breaches were processed at the Community Justice Services (CJS) Centres by Community Corrections Officers (CCO) (most people would know these as “Parole Officers”). The establishment of the CBU centralised the breach process and all paperwork was now to be handled by the same small group of people based in an office on St Georges Terrace instead of individually by different officers dotted throughout the State. The idea was to specialised and streamline the breach process.

### **The Struggle Begins**

When I started the evaluation, CBU had been operating for nearly two years. The evaluation had been scheduled as part of the project management process when the Unit was first established. The main aim of the evaluation, not surprisingly, was to find out whether the CBU was making it quicker and easier to breach offenders.

There are some obvious quantitative questions that you would want to start with when beginning this evaluation:

- How many breaches occur each year and how long did they take to process;
- The rate of breaches for re-offending versus breaching for non-compliance with conditions; how many male/female, Aboriginal/ non-aboriginal offenders.

It would also be useful to know the outcome of the breach process, e.g.:

- How many breaches resulted in new orders;
- How many resulted in a fine, and;
- How many offenders ended up being sentenced to a term in custody?

You would expect that these simple questions could be answered with the available statistical data. Not so. About six months before I started the evaluation, a brand new Department-wide computer system was introduced to collect and make available a range of information about offenders on community corrections orders. This new system is called the Community Business Information System or C-BIS. With regard to the collection of data relating to community corrections orders there were some initial problems with the new system. These occurred on two levels. One was due to the high level of data entry error that occurred initially as staff became acquainted with the new system. The other was due to technical weaknesses or gaps in the actual system itself which allowed the high level of human error.

With regard to the information relating to breaches, these initial teething problems introduced a margin of error to that year's statistics that was pretty much equal to the expected numerical variations within the data. In other words, the margin of error was roughly the same, and in some instances greater, than the expected change in figures from one year to the next. I worked

this out by looking back at the data over the previous six years. The first five of these years were prior to the introduction of the new computer system, and in each of these years the figures varied by two or three percent. The year after the new system was introduced the figures also varied by a few percent, but in a positive way that would suggest the CBU was having the desired impact. For example, the number and rate of re-offending breaches decreased while the number and rate of non-compliance breaches increased. This means that more offenders were being breached for non-compliance before they committed an additional offence. This would be a positive evaluation finding because it suggests an improvement in the case management of offenders that might be attributable to the Central Breach Unit. At least, it would have been a positive finding if I had been able to rely on the statistical data, but I couldn't.

### **Zeroing in on the Problem**

When I asked our data team to pull out the breach data for me, I asked for 35 different data fields. This included information such as the year, offender ID, type of offence, prison location, date of breach action, court date, court outcome, etc. I discovered the data error when I tried to combine fields that included data that would have been entered at the CJS branches with fields using data entered at the Central Breach Unit. The two sets of data were entered at different points of the breach process into different types of screen queries. While each user was adding data to the system, the basic details e.g. dates, type of breach, offender demographics etc, should have been the same; but they weren't. This is what was making the data unreliable.

The data errors were pervasive. They ran across all data fields from the number of offenders breached to the type of breach (non-compliance or re-offending) to ethnicity and gender. The margin of error was even greater in the data relating to the outcome of the breach process and the amount of time that had elapsed between the breach commencing and an outcome being obtained; my key evaluation questions!

In the end, we managed to calculate the total figure for the number of breaches that occurred during C-BIS's first year of operation with a good deal of confidence, but that was it. All the other information was unreliable. Even though the data were consistent with expectations with the introduction of the Central Breach Unit, none of it could not be used with any confidence for the purposes of evaluation.

Eventually, I gave up trying to make sense of the inconsistencies in the data. I just had to accept that it was bad luck that a new computer system was introduced just as CBU might be starting to have an impact on departmental statistics. I still included a statistical analysis with the evaluation report, but it came with a massive caveat.

By this stage I had spent several months working on the evaluation but had produced no useable outputs. I had to rethink my whole strategy. I had to work out how I could put all the work that I had done so far to good use and how I could give the public a good return on its dollar.

### **Why Am I Doing this Anyway?**

One of the reasons why I am attracted to evaluation rather than pure research is the idea of being genuinely useful at a practical level. Not the 'contributes to our understanding of the field' type of *useful* that you do with your Ph.D., but on the ground, make it easier for people to do a good job, type of *useful*. Another reason why I am attracted to evaluation is that I hate it when

people waste public money. It infuriates me when people throw money at ill-thought out projects and programs that sometimes do more harm than good. And, it frustrates the hell out of me when people carry out, or commission, expensive evaluations that may be technically sound but produce very little insight that will actually help improve program delivery. I was determined not to let this evaluation of the Central Breach Unit turn into a waste of time and money.

### **I'm Nothing if Not Flexible**

In the end, I figured that someone was going to have to sort out the Unit's data problems and, given how deeply immersed I was already, it might as well be me. If I could help the Department strengthen its data collection systems and provide more accurate information about how offenders were being managed in the community, this would represent a valuable and tangible evaluation outcome. At this stage I also recognised that the paucity of quantitative data meant that I would need to rely more heavily on the qualitative data. I had already planned to conduct a limited number of semi-structured interviews of staff from the Central Breach Unit and from the field offices. The change in my evaluation strategy would mean a lot more, and a lot more in depth, stakeholder interviews.

So my evaluation changed dramatically, as did my role. Up until now I had played the role of statistical analyst and then systems analyst – although I use that term very loosely. But my evaluation was to change completely, from a statistical based *impact evaluation* to a *process evaluation*. I now needed to start looking at the actions and procedures of staff in the field to work out where the human error was occurring and why. I figured, if I had to start looking at processes anyway, I might as well make it a comprehensive look and expand my scope beyond an explanation for the lack of data integrity. So I went back to the senior manager that had requested the evaluation in the first place and discussed with him the prospect of a dramatic change in the evaluation's scope, methodology and core objectives.

My role as an evaluator was now becoming something akin to a business analyst or trouble shooter. My new focus meant that I needed to examine existing procedures in great detail, both as they were intended and how they were actually being carried out in the field. I needed to look at how data were being entered into the system and at what stage in the breach process in an effort to locate the source of several consistent data entry errors. And I needed to talk to field staff, both at the Central Breach Unit and the CJS branches to find out why they were entering the data the way they were. Once I started talking to staff in the field, the evaluation changed again; and so did my role.

### **Communication is Everything**

In every evaluation I have ever done there is one particular issue that crops up with frustrating consistency: communication – or lack thereof. The case was no different with the Central Breach Unit. The project document analysis, coupled with the field interviews, had revealed that staff, at both the CBU and the CJS branches, were routinely engaging in actions that served to undermine the objectives of the CBU. The CBU was set up in an effort to speed up the breach process, but staff were regularly doing things that were slowing it down again. In many instances, these practices were a direct result of a lack of communication between staff at the CJS branches and staff at the CBU. What was happening was that staff at the CJS branches were doing things in a certain way because it helped them meet *their* objectives as quickly and easily as possible. Staff at the CBU were then re-doing things so that they could meet *their* objectives as quickly and easily as possible. Neither of them was looking at the big picture. Neither of them was looking at the breach process as a whole. They did not look past their own area of responsibility.

Neither group had a clear idea of what the information they entered into the computer system was used for by head office. They did not realise that the data they entered was being used to produce regular monitoring reports and that it was being used regularly to brief the Corrective Services Minister. Neither of them realised that even the date on which they entered their data, would have an impact on performance monitoring.

During the field interviews it became clear that staff at both the CBU and the CJS centres were acting in a way that was perfectly logical, if you were only looking at their area of responsibility. It was only when you looked at the breach process as a whole, that you could see how their specific actions could be causing unnecessary delay. And we are talking about very basic things here, such as regional Courts faxing documents to CBU when original certified copies are needed, or Community Corrections Officers recording Court outcomes based on what they heard in Court and sending that to CBU rather than waiting for the more accurate data to be entered into the Court database. These things are not rocket science, they are simple procedural issues that could be easily adjusted with no additional cost and would result in significant savings in time.

The practice of redoing each other's work without actually speaking to each other was creating tension between CBU and the CJS branches. A rift was beginning to develop. The myriad of minor procedural inefficiencies were not the biggest problem, they were a symptom of it. The biggest risk to the CBU being able to achieve its stated project objectives was the lack of communication between staff at CBU and the CJS branches. So now my role as a business analyst, turned into that of mediator.

### **I'm Not the Expert Here**

Having identified a relatively long list of minor procedural inefficiencies and errors, I now had to work out how to remedy them. I have worked in this Department for about four years and I know basically how it operates. But Corrective Services is a massive organisation and I still know very little about the intricacies of daily operations at each of the field offices. As an evaluator I could spot the problems, but I was not in a position to be able to resolve them... well, not on my own anyway. This was particularly true with the CBU because there were legal requirements underpinning most aspects of their procedure.

This meant that the solutions had to come from field staff. They were the only ones in the position to know what would work and what wouldn't. Which bits of their procedure were legally required and which could be modified. They also knew the history behind their daily practices, how certain shortcuts had been developed and why.

Usually, when your field interviews reach saturation point, when you are no longer learning anything new from your respondents, you would consider this stage of the evaluation to be complete. I didn't do that in this case. What I did instead was continue to meet with staff and used this as an opportunity to not only confirm the issues but also to brainstorm possible solutions. Once I had gathered a range of possible solutions that all looked sensible to me, I then took them back to the relevant managers to test their feasibility.

By the end of the interviews I was able to put together a table outlining the key issues and problems along with the potential risk they posed, and also make a number of clear, tangible, and feasible recommendations towards their resolution. The final report, and the table of key findings and recommendations, contained no surprises. All of the solutions identified in the report

had either been put forward by field staff or had been discussed by them. Any impractical solutions had already been eliminated through the brainstorming interview sessions and through discussions with management. More importantly, the necessary compromises had already been reached. The debates had already been had. The only recommendations that made it to the final report were those that stood a very good chance of being implemented because they were 'owned' by both field staff and the relevant managers.

In the end, there were 18 recommendations made in the final evaluation report. Of these, 17 were supported by the senior executive. CBU implemented all of the recommendations for which they were responsible. The only recommendations that were not immediately implemented were those requiring large-scale changes to the computer system. These items were added to the system's reform agenda, but no concrete timeframe given for their implementation.

### **What's the Moral of the Story?**

When I first started having trouble making the statistical data in the Central Breach Unit evaluation add up, I panicked. I kept re-jigging the data over and over in an attempt to get hold of some figures that made sense and could be used with at least some semblance of reliability. I spent a lot of time, too much time probably, on that data. Worse still, I felt like the evaluation was *failing*: that I was wasting time without producing anything meaningful.

It wasn't until I took a step back and looked at it from the other side of the equation that I started to feel that I could do something useful. I asked myself what I would want from the evaluation if I was senior management and it was *my* project being evaluated. What would I want from the evaluation if it was *my* workplace being evaluated? What would I want from the evaluation if it was *me* who was under a community based order?

In the end, I realised that neither senior management, nor the staff at the Central Breach Unit and the CJS branches, nor the offenders serving their sentences in the community, were going to be concerned about the computer glitches that prevented me from getting the data I needed to conduct a technically proficient statistical evaluation. What they cared about was how what *I* was doing was going to affect what *they* were doing. Was the evaluation going to make their lives harder or was it going to make it easier?

I very much wanted to make their lives easier; and to do that I had to be flexible. I had to work with my key stakeholders to find out what I *could* do for them that would be useful instead of going with my initial instinct, which was to dress up the faulty statistical data to make it look pretty even though I knew that it would be of little practical use to anyone. In the end, I conducted a completely different evaluation to the one that I had first planned. In the end, I felt that I had really had made a difference. I had helped to make a tangible improvement to the breach process.

It was a good outcome all round.