Exercise: Privacy & Security Awareness, Education, and Training

CPNI have provided funding to ACME Water to enable them to make their work diaries electronic.

Rather than updating a physical logbook, plant operators will now add events to electronic diaries running on their ICT PCs. Each entry will be logged against operators' "pay number".

A condition of the funding is that ACME Water will provide periodic copies of work diaries; this will facilitate the analysis of anomalies for potential national threats to the water infrastructure.

Questions

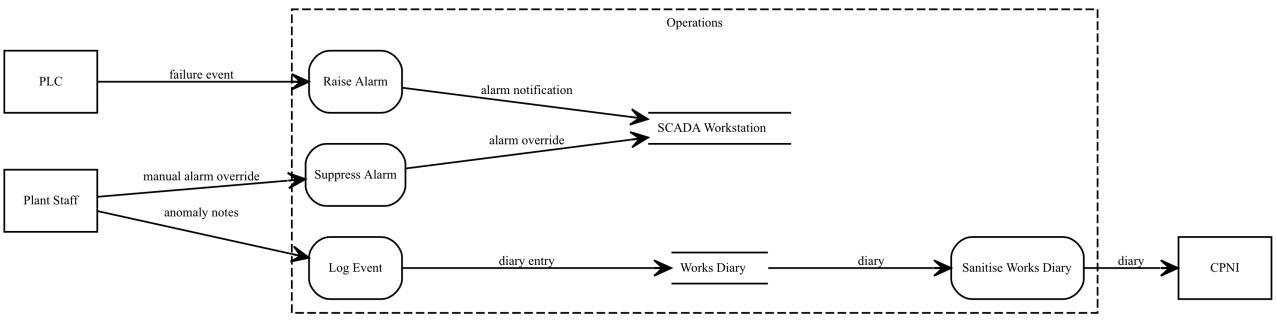
1. Because the Diary Event asset now contains personal data, revise the ACME Water model provided to:
   - model diary events as personal data,
   - add new model elements to capture the flow of data from ACME Water to CPNI for anomaly processing,
   - identify any new privacy risks associated with this change,
   - revise the 'Day' policy goals to incorporate new privacy requirements introduced by this change.

You may find it helpful to periodically validate your CAIRIS model (from the Models/Validate menu) to check for any issues.

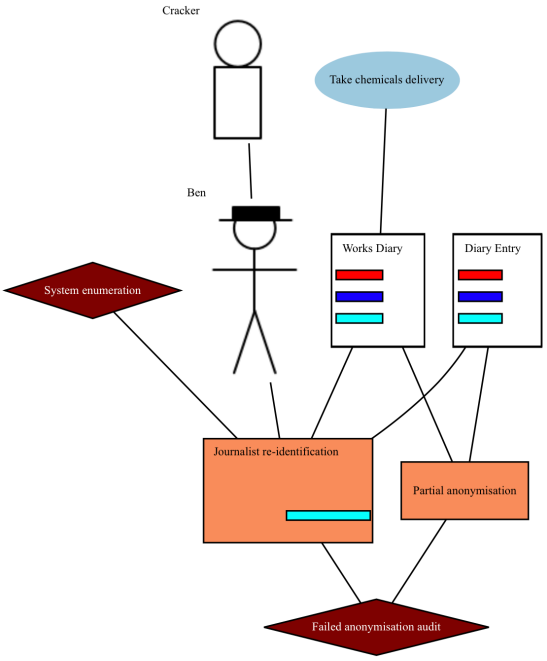
The ewd.xml CAIRIS model (which you need to import on top to the ACME Water model) illustrates what a model with these changes might look like.

To model any personal data, Data Controller and Data Subject roles also need to be defined. In our model, we define the pre-existing Information Security Manager role as a data controller. However, as there needs to be some form of sanitisation process then the Machine role also needs to be defined as a data controllers. The Plant Operator should be set as a data subject. Once these have been defined, dependency relationships between these roles (dependers) and plant operators (dependees) can be added to represent informed consent and identify the Diary Event asset as personal data. However, when validating the model, you should find that the Works Diary also needs to defined as personal data too.

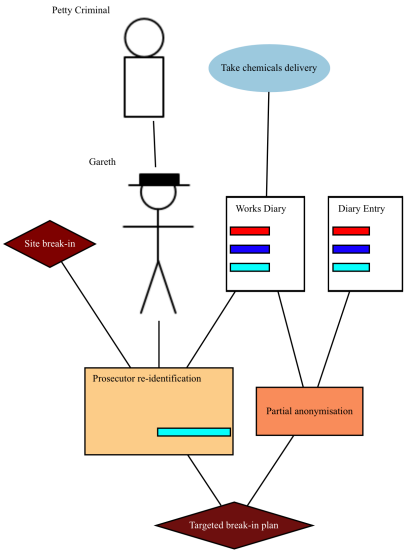
The figure below illustrates the revised DFD with a new 'Sanitised Works Diary' process.



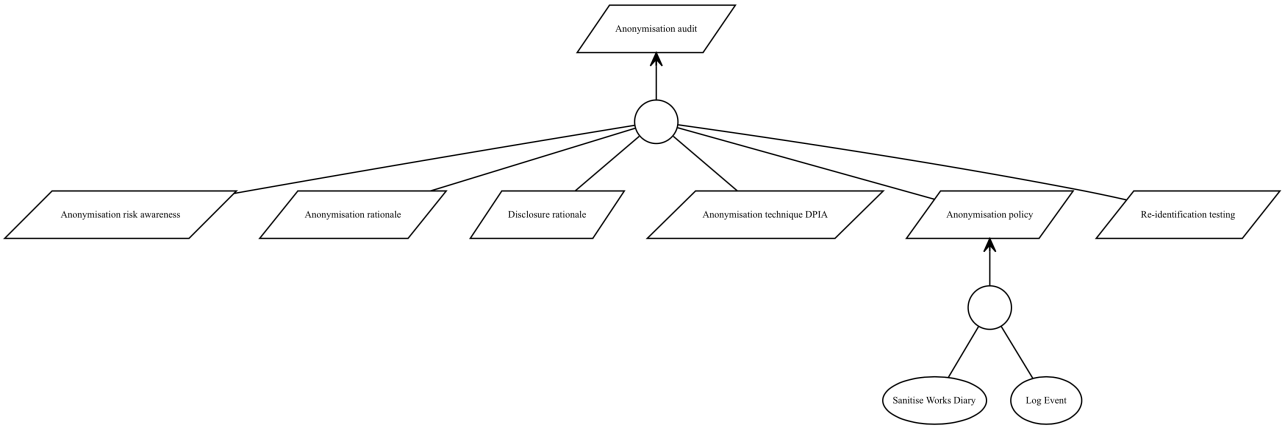
There are a number of re-identification threats against anonymisation, but our model focuses on two risks in particular.



The first is a failed anonymisation audit as a result of Ben carrying out a Journalist re-identification threat based on partially anonymised diary data. As you'll see from the risk model, the threat is made possible by a pre-existing System enumeration risk where Ben was able to access pre-existing database instances. The misuse case for this latter risk indicates this, but — in the original ACME Water model — the Works Diary was physical. In our revised model, this asset should now be associated with the Enumeration threat.



The second is a targeted break-in to an ACME Water site; this is facilitated by a Prosecutor re-identification threat, again based on partially anonymised data. In this case, however, Gareth is using pre-existing knowledge he has on ACME Water staff based not only on data previously collected but personal knowledge of plant staff.



To incorporate the privacy requirements mandated by this change, we add a new Anonymisation Audit goal; this a refinement of the pre-existing Compliance audit goal. To satisfy an Anonymisation audit, several other goals need to be satisfied. These goals are drawn from the ICO's Anonymisation code of practice. Notice that one of the goals is operationalised to two use cases/processes that handle personal data. This indicates that the processing is 'necessary' with respect to the UK Data Protection Act.

2. As part of your budget, ACME Water have invested in several copies of *D0x3d*. Based on your understanding of plant operators, how might these games help satisfy your new privacy requirements?

The game can help satisfy the Anonymisation risk awareness goals in a number of ways:

* *As a serious game, d0x3d uses fun as an outreach tool. In this case, the game is putting in context the different ways PII might be protected and collected.*
* *d0x3d omits a lot of technical detail, and doesn't require much technical background.*
* *d0x3d surfaces the need for people to discuss issues and start conversations that otherwise might be avoided; this can help overcome any inappropriate folk knowledge people might have around security and privacy.*
* *d0x3d is unobstructive. It doesn't require any computer labs and, in principle, is quite and easy to setup. In practice, people would need to take the time to learn the rules, which are not intuitive to complete novices.*
* *d0x3d is open to modification but, again, this would require time and resources.*

It's less clear how d0x3d can help achieve the other privacy goals. Like any SEAT intervention, the game would need to be situated around those receiving the content. Given the main beneficiaries are plant operators then one challenge will be finding an opportunity for plant operators to play the game together - no mean feat given they work shifts!