****

**The objects and aims of the Consortium of European Research Libraries (CERL) are to provide services to its members and to the library and scholarly world at large in the form of bibliographical databases, seminars, workshops, publications and co-operation with other library organisations and individual libraries and their staff. CERL concentrates its efforts on printed material from the hand-press period – up to the first half of the 19th century – and on manuscripts, both in analogue or digital format.**

*[excerpt]*

**Using the Collection Security questionnaire: the example of the Royal Library of Belgium**

[www.cerl.org/services/seminars/previous\_cerl\_annual\_seminars](http://www.cerl.org/services/seminars/previous_cerl_annual_seminars)

The Working Group of the Security Network finalised a collection security benchmark questionnaire within the framework of the Fourth LIBER Collection Security conference in The Hague in November 2012. The institutions of all the group members took part in this survey. The results were delivered in December 2013. The Royal Library of Belgium has tested how to use the results as a basic audit and thus as a valuable source for promoting projects which directly or indirectly enhance collection security.

|  |  |  |  |
| --- | --- | --- | --- |
| Physical security | | | |
| N° question | Yes (%) | No (%) | In part (%) |
| 64 | 40 | 30 | 30 |
| 65 | 80 | 0 | 20 |
| 66 | 60 | 10 | 30 |

The questionnaire resulted from of a concerted exchange of ideas inside the group including the larger national institutions, so we can take it as read that the questionnaire covers the aspects which are essential to meet the needs for the security of our collections. That notwithstanding, we thought it is important to keep in mind that zero risk does not exist and that risk analysis cannot be fixed; this obliges us to stay vigilant and creative, continuously adapting and improving our procedures. The questionnaire contains around one hundred questions divided into six topics - governance and policy, access and use, physical security, staff and processing areas, collection management and finally exhibition and transport - so it really constitutes a significant auditing tool. The questions were formulated so as to obtain the answers ‘yes’, ‘no’ or ‘in part’. 76% of the questions were answered ‘yes’ by a minimum of 50% of us (91% by min 30% of us, 47% by min 70% of us) and none of us answered ‘no’ to 47% of the questions. Bearing in mind that the questions were formulated so that the answer ‘yes’ is positive for collection security, this shows the relevance of each of the issues addressed by the questions. This can be crucial when using the questionnaire to argue for projects within the institutions. The results suggest that we might consider the questionnaire as a standard guideline. Within such a simple system, when you present the overall results for each question of each domain one below the other (all institutions taken into account - see example at the end), simply colouring the column that corresponds to your answer - in green for ‘yes’ , red for ‘no’ and orange for ‘in part’ – provides an immediate overview of the proportion of questions you have answered ‘yes’, ‘no’ or ‘in part’, with, as a corollary, a relatively accurate representation of your situation. You can directly point to the topics where you show weakness, and get an initial idea of the problems you have to tackle.

To go further, however, the evaluation must be refined. It would be wrong to focus only on the questions for which you answered ‘no’ or ‘in part’. The questions answered positively also require analysis. Were you sufficiently critical when you answered? Are the existing solutions mature enough or really efficient? We have a duty to question some ‘confirmed’ solutions. We must adopt the new trend of admitting and learning from our failures as it happens nowadays in business and industry. You have to prioritise the problems that need to be addressed. At this level, the global results represent a significant help: a rule implemented within 80% of the institutions can either be considered as merely easier or as more significant than one implemented within only 20% of the institutions. Then you have issues such as whether the achievement of the solution is 100% within your control or not, the degree of difficulty, the cost, etc. When you deal with the questions you answered ‘in part’ you can analyse the reason for incompletion, determine if the partial solution suffers from a lack of harmonisation or, more difficult to admit, you have to recognise that the reason why you cannot extend a rule to have wider validity is because it is inadequate.

Now, as the work to be accomplished can be sizeable, it’s important to take certain aspects into account. First, we are not alone! The biggest institutions can certainly help, advise or inspire smaller ones. Taking an active part and daring to confront the issues is also important. All of this can be achieved through groups such as the security network. It is essential to avoid reinventing the wheel: sharing documents, forms or similar can lead to substantial savings of time and money.

Next, it would be a significant loss of energy and resources if you tackle problems without having a really good understanding of the environment. You must develop knowledge of your building that is as in-depth as possible: without this it is impossible to protect it. You also have to know what the means at your disposal are internally as well as externally, whether budgetary or from a human resources point of view. Forgetting the psychological aspect would also be a source of failure. Being conscious of the internal brakes towards changes, promoting the maximum participation of staff and investing time in education and communication is essential to guarantee comfort, acceptance and motivation. Promulgating a perfect rule without having the means to apply it would be absurd. It is better to get a less ambitious one which you have the means to apply properly and completely consistently.

Finally there are needs for security that encounter those for safety, preservation and conservation. It is important to spot those meeting points because it considerably increases the possibilities to convince other people in the organisation and to find support of any kind.

*Jacqueline Lambert, Royal Library of Belgium, Brussels*

*[end of excerpt]*