HealthManagement
Promoting Management and Leadership

Volume 15, Issue 2/2013 - Medtech

Information Security Consultants in Hospitals: Is Outsourcing the Answer?

By Koen Claessens

Since the establishment of the Crossroads bank of Social Security in Belgium in 1990, it is a legal requirement for all organisation receiving access to the bank to appoint an information security consultant. By this assignment, they would also comply with the European data privacy legislation. In practice, a lot of hospitals are not able to find such a consultant and assign them with a meaningful job description for several reasons.

In the beginning, only few security consultants were appointed because no consequences were linked to non-compliance. On July 5, 2011 however, the sectorial Committee on Social Security & Health in Belgium decided that hospitals without a consultant would no longer be granted access to personal data of the Crossroads bank and national register. An important underlying reason for this decision was the increasing computerisation in hospitals, especially when it comes to patient medical records and the electronic exchange of data, which increases the risks concerning data privacy even more.

In the future it is expected that the requirement of a security consultant will be enforced in other types of organisations that manage personal data. In the social security sector this would for example apply to pension funds, insurance companies and social secretariats.

Lack of Budget and Appropriate Candidates

Many hospitals have problems filling out the requirement of an information security consultant. First of all no budget has been foreseen by the government to support this new requirement. As a consequence, often a cheap solution is sought. Also, hospitals often have difficulties finding an appropriate candidate within the organisation or by recruitment, who has the required knowledge and motivation. This is especially difficult given the fact that the security consultant must be independent and therefore may not be part of the internal IT department, where the required knowledge is strongly IT oriented.

In the meantime hospitals have developed a variety of models to fill out the function of security consultant. For example, six psychiatric hospitals are collaborating by sharing the same security consultant. This is possible because the six hospitals use similar software so combining efforts and working with one security consultant is more efficient. Two other hospitals are using a “cross-fertilisation strategy”, the IT manager of hospital A is security consultant in hospital B and vice versa. This might also enable synergies between both hospitals in the future.

Startup Tasks Versus Recurring Tasks

The functional description of an information security consultant reads as follows: ‘He/she advises the Executive Director concerning all aspects of information security. This implies a documenting, analysing, advising and monitoring role. He/she designs security plans for a certain period, which incorporates the resources required to execute the plan. It is therefore not an executive or management function, the responsibility concerning actual decisions about information security entirely lies with the management.’

In other cases where an internal security officer is assigned, hospitals often have difficulties to assign a meaningful and substantive interpretation to the tasks of the security consultant. And even when the government organises seminars concerning this issue, they are often not sufficiently pragmatic to define a concrete approach and project plan for the security consultant.

The tasks of the security consultant can be divided into two different groups. On the one hand there are ‘startup tasks’, which consist of establishing an information security policy, performing security risk analysis and designing the security plan based on this. On the other hand, there are also ‘recurring tasks’, which are to be executed on a regular basis. These include for example the monitoring of and responding to security incidents, the reporting on the progress of the security plan and keeping all security documents up-to-date.

Outsourcing Ensures Independence

Given the fact that the function of security consultant is neither an executive nor a management function, but rather an advisory function, the position is well suited for outsourcing. Furthermore, the outsourcing of the function ensures the independence of the security consultant. As external advisors, they dispose of the necessary competences in the field of IT, information security, documentation and analysis.

Author:

Koen Claessens

Partner
BDO
koen.claessens@bdo.be

Published on : Fri, 24 May 2013