ITMAGAZINE

Information security evaluation: a holistic approach

9. Dezember 2012 - *By Igli Tashi, Solange Ghernaouti-Hélie.Management of Technology Series. EPFL Press 2011*

Context and scope

You can only have real confidence in your information security programme if it's based on a strong foundation and if it has been developed with conviction. The main challenge for security practitioners is to increase the level of trust over their business partners and stakeholders believing that their business is protected by a robust information security practice.
In order to capture the intent «to be appropriately and commensurately» protected, an evaluation should be based on a targeted assessment, aligned with the organisation's business needs. In doing that, an information security function should have a consistent and coherent structure, operate as expected, and respond to specific business needs.
This book presents a global, systemic, and multidimensional integrated approach to the holistic evaluation of the information security posture of an organization. It is based on, and integrates, a number of information security best practices, standards, methodologies and sources of research expertise, in order to provide a generic model that can be implemented in organizations of all kinds as part of their effort towards the improved governance their information security.
This approach contributes to improving the identification of security requirements, measures and controls. At the same time, it provides a means of enhancing the recognition of evidence related to the assurance, quality and maturity level of the organisation's security function thus driving improved security effectiveness and efficiency.

The problem

Executives, in spite of all the papers and theories published in hundred of books and newspapers, still have a limited view of the importance of the information security practice. Fundamental questions with regards to the position of the information security within the value chain of the organization, as well as the nature and the extent of the resources and efforts dedicated to it, are very often considered a posteriori. The PwC 2012 Global Information Security Survey outlines that the lack of an actionable vision or understanding from Executives is identified as one of the greatest obstacles to effective information security from a strategic point of view. This is the case for 37 % of the CISO and for 30 % of CIOs that responded to the PwC's security survey. Executives are motivated by the fear or after the occurrence of a crisis, but when problems arise this is unfortunately too late.

The approach

The Information Security Assurance Assessment Model (ISAAM) can be used to evaluate the information security posture in a given period of time and aiming to provide a faithful picture of the protection level achieved by being as pragmatic as possible.
In doing that, ISAAM uses a system based on a triple evaluation aiming to quantify the level of trust that can be put into a given subject of the evaluation (a security measure or process) as well as into the security system as a whole. This is the result of three different evaluation angles, namely
- the resilience of the security structure;
- the quality of the security processes; and,
- the level of the alignment of the security practice with regards to the business objectives.

ISAAM's structured assessment approach enables organizations to perform a holistic assessment of their overall security protection system rather than the traditional piecemeal or compliance-driven evaluation approach. This rigor makes the assessment much more valuable to the organization by reducing the complexity arising from the number of security safeguards and practices, and the evaluation methods of a multiple nature and scope.
ISAAM focuses more on the consistency of the security practices in place and the related constituent elements of security rather than on their overall compliance level against a single best practice or methodology. To holistically evaluate the

information security program, ISAAM clearly sets out the various relevant multidimensional aspects of information security. This enables us to identify the specific concerns and safeguards put in place to address those concerns. As a consequence, the level of confidence senior management can expect from their information security programme by assessing the four dimensions against the three evaluation axis, is related as previously mentioned to the capability to respond and quantify the output of the following:
- Resilience of the structure: is my security programme consistent and coherent over all the dimensions?
- Quality of processes: is my security programme delivering as expected?
- Maturity level of the programme: is my security programme aligned with my expectations and business needs?

The solution

The holistic evaluation based on the methodology proposed by ISAAM, will allow organizations to obtain:
- a greater and a more meaningful understanding for senior business decision makers over their security practices;
- the gap between security performance that
is put in place for their specific business needs ; and
- continuously monitor and improve their information security position.
The added value of the ISAAM evaluation approach is that it is easy to implement and operate and it addresses the concrete needs of the business in terms of reliance on an efficient and dynamic evaluation tool, using a coherent system of evaluation. This book gives to the Executives, for whom information security is a priority, a valuable tool, based on a global and integrated approach for information risks and security management and also enables them to effectively run the information security function within their organization.
Igli Tashi: PhD in Information Systems / Master of Advanced Studies in Legal Issues, Crime and ICT Security /expert on information security and risk management at PwC
http://www.pwc.ch

Solange Ghernaouti-Hélie: PhD in Computer Science / professor of the University of Lausanne / founder and director of the Swiss Cybersecurity Advisory and Research Group
http://www.hec.unil.ch/sgh/