

Information security: security to match a company's issues and risks

> Controlling your security risks at all levels of your IS

Issues related to security risk analyses are common within companies.

However, this frequency is accompanied by a multitude of methodologies and areas for analysis, the performance of which can vary greatly. Using its experience, Beijaflore has built an approach to address this type of subject, avoiding known pitfalls.

Security risk analysis allows security vulnerabilities to be mapped and prioritised. It involves estimating the vulnerabilities of the examined system, the potential for occurrence of internal and external

threats, and their business impacts. This prioritisation makes it possible to target security efforts, optimise investments, and become better aligned with business issues.

However, companies face several challenges when they perform their security risk analyses. First of all, the view of the technical departments is often uncorrelated with that of the business area. Then, there are often inconsistencies between the results of various risk security analyses conducted within a single organisation. Lastly, companies struggle with existing methodologies, which are too generic or comprehensive.

> Consider business specifics to adapt risk analysis tools

To ensure the relevance of the results of a security risk analysis, it is essential to return to the business context. Taking the company's characteristic information into account makes it possible to adjust the various activities of the process. This adjustment guarantees, among other things, consistency with other future analyses and pertains to the elements making it possible to supervise and conduct this exercise, namely:

- **The catalogue of securities risk classes**, which must be expressed in a language that can be understood by the business area, relying on existing catalogues (e.g. mapping with the "Basel II" risks);

- **The considered attack scenarios**, which should benefit from formalised lists of attacks in the known frameworks (like "EBIOS") and propose an appropriate selection of them in the IT and business context;

- **The scales of potential and impacts**, the levels of which are to be refined in order to take into account the business area characteristics specific to the company (in legal, financial, or image terms, for example).

By integrating the business challenges and adapting these three elements to the company's context, the results of the risk analysis are aligned with the business area and thus facilitate decision-making and risk control.

> Extracting historical information related to the risk potential and impact

To ensure that the results of the security risk analysis reflect operational reality, factual elements must be provided to support the thinking:

- The history of security incidents having occurred;
- The list of open audit recommendations;
- The list of known vulnerabilities (vulnerability scanner not filtered, for example);

- The regulations applied to the business area (e.g. Basel II, Data Privacy).

Corroborated by these elements, the estimated potential and business area impacts will be in line with the operational reality of the company.

> Using business area and IT expertise to unify the view of the company's security risks

The next step involves identifying the people in the company who have a good view of the business area and its challenges as well as those mastering the IT infrastructures and their level of security maturity. As well as the risk analysis sponsor, whether it is the IS security manager or the Compliance manager, others may be called upon to provide their expertise and knowledge of the known risks of the company. These people can be part of operational security, internal audit, or the network and can be involved during two separate workshops.

The first, business-oriented, primarily allows the impacts of each risk class on the business area to be estimated. These risks can be analysed

according to the previously determined impacts (financial, human, image, for example).

The second, IT-oriented, focuses on methods of attack that could lead to the generation of one or more risk classes. The objective of this workshop is to determine the potential for the occurrence of these attacks by taking existing security measures into account.

Once consolidated, these results are validated in a committee by the stakeholders. The results make it possible to present identified security risks in a language adapted to the business area and define, from an IT standpoint, the possible associated action plans to be implemented.

> Having the residual risks validated by the business area and adopting an appropriate treatment plan

With security risk mapping completed, several options are available to the business area, the owner of the risk:

- Retention, which involves accepting risk as is;
- Reduction, also known as mitigation, which aims to reduce the level of risk (e.g. implementation of additional or improved security measures);
- Transfer, designed to put the risk on a third party,

without a transfer of responsibility (e.g. transfer to an insurer);

- Refusal, resulting in the removal of the risk's causes in most cases (e.g. project suspension).

The risk treatment plan must be validated by the business line, which accepts the resulting residual risks. ■