National Cyber Security Centre
Ministry of Justice and Security

Risk management: the value of information as point of departure.

On ownership and responsibilities

Factsheet FS-2020-04 | version 1.0 | july 9th 2020

Incidents involving important and/or sensitive information can have a serious impact on organisational objectives. For this reason, ultimate responsibility for effective management of the risks associated with information lies with the board. Line managers are responsible for the tactical and operational risks associated with the information that is processed within their department. In order to manage risks, they must be carefully identified and assessed. If you want to identify and manage information-related risks, you must first identify and manage the information itself. Make sure, therefore, that ownership of the information itself and the associated responsibilities are clear as well.

Background

In the information-driven society in which we live, we process a huge amount of information. Although we are in many cases dependent on this information, it can also pose a risk to your organisation or to others. Some risks offer opportunities; others can lead to extremely serious incidents. This latter category of risks must be managed. The more important or sensitive the information or the greater the consequences of an incident, the greater the need to manage these information-related risks.

Target audience

This fact sheet is aimed at the board, management and the CISO of organisations that want to identify and manage the risks associated with working with information.

Cooperation-partners

The Brabant water boards, CISO Masterclass BV, Digital Trust Center (Ministry of Economic Affairs and Climate Policy), the Rijnland water board, the Netherlands National Communications Security Bureau (General Intelligence and Security Service) and Octopus-IB.

The issue

Organisations depend on information to carry out their core activities. Unfortunately, however, they are not always sufficiently aware of the value of this information, either to themselves or to those with malicious intent. This lack of understanding means that organisations fail to focus sufficiently on identifying and managing the risks that occur when working with their information.

Managers are responsible for the availability, integrity and confidentiality of information in their processes. At the end of the day, they are the ones who will suffer the consequences of incidents involving their information. However, they do not always take this responsibility seriously.

In this fact sheet, we talk about the 'board', by which we mean the top management body in an organisation. Your organisation may call it something different. For the sake of simplicity, we use the term 'board'.

The form that effective risk management will take will vary from one organisation to another. Embrace the message about organising the ownership of information and the associated risks and specifying the related responsibilities, filling in the details according to your own specific requirements where desirable or necessary.

The problem

In recent decades, the volume of information that we process has increased considerably. In addition, the opportunities offered by digital technologies have enabled us to link more information together. As a result, the processing of information has also become more complex. These two developments make the management of information extremely challenging. However, the extent to which we focus on the management of information has not kept pace with the growth in the volume, complexity and importance of this information.

The use of IT makes it difficult to obtain an overview of information. With a filing cabinet or archive, everyone can see how much information is stored there and where it is filed. To do this for an IT system, you need IT knowledge, which many people do not have. If that IT system is in the cloud, it is even more difficult to determine what is where.

Nowadays, information and information technology are inextricably linked. In the old days, the means by which information was recorded (typewriter, printer, paper, binding, etc.) were simpler and we did not place great demands on them. In today's world, things are different. Digital means must be faster, more user friendly, more attractive and more portable. They must also have more functions and be available at all times. We therefore pay far more attention to the means than we did in the past. As a result, information no longer stands alone but rather has become part of the means.

This limited focus on the information itself and major focus on the means is also evident in the field of information security. We focus too much on technical security measures and the technical side of digital attacks and too little on the value and importance of our information.

We will look first at how to identify and manage information and then at how to identify and manage the risks associated with this information.

How do you identify and manage information?

If you want to identify and manage information-related risks, you must first identify and manage the information itself. Recognising that information is an asset that requires active management, just like personnel, stocks and finances, for example, will help in this context. Since information is used by the entire organisation, the entire organisation must be involved in the strategy employed to manage it. This strategy will include the following steps.

Role of the board

For the strategy to be effective and long term, the involvement of the board is crucial. An organisation is just as dependent on information as it is on labour, capital and natural resources. The board must manage information as a production factor in its own right and promote this attitude among the entire organisation.

Ownership of information

For information to be managed effectively, all information must have an owner. Ideally, this will be an explicit owner, not an owner derived through ownership of the process. This is because information can be used, copied, linked, etc. in multiple processes, which can lead to a lack of clarity over who is the actual owner. In the case of an incident in particular, it is important to be clear immediately as to who is the owner.

Line managers are the obvious candidates to be information owners. They are responsible for day-to-day management of the organisation, in places where, if information is not reliable or available, there will be a direct impact. In order to ensure that information is managed effectively, the board must hold information owners accountable for the fulfilment of their responsibility.

Making someone the owner of information does not automatically mean that that person has the right knowledge to be able to take that responsibility. Consequently, where necessary, owners must be given the appropriate support from the information management department.

Information management

Effective information management requires specific expertise. The organisation must therefore have the necessary understanding of information management. Information management will supervise and provide the support required to ensure that information is managed effectively. In other words, the information management department has no control over the information. That responsibility lies with the information owners.

In order to ensure that the management of information within the organisation is standardised and to clarify exactly what is expected of information owners, information management must have direct access to the board and an information policy that has been agreed with the board must be in place. Although information is generally processed using information technology, information is not part of information technology. Consequently, positioning information management within the IT department is not advisable. Information is an asset in its own right and information management therefore deserves an independent position within the organisation as an independent department.

The CFO under the IT manager?

Locating information management within the IT department based on the argument that information is always processed on a computer is not advisable. If you use that argument, the finance department should come under the IT department as well, because financial transactions nowadays are almost always done on a computer.

Identifying information

For information to be managed, it must be clearly identified. The primary and other key business processes constitute a good point of departure for producing an overview of the relevant information within an organisation. The information management department is the obvious candidate for coordinating the mapping of the information landscape.

The identification of information must not be limited to information within the organisation. Information for which the organisation is responsible may be stored with external parties. The organisation may also, to a certain extent, be dependent on information from external sources. Make sure you include this type of information in the overview.

Article 30 of the General Data Protection Regulation requires controllers to maintain a record of processing activities. Rather than a record of the processing of personal data alone, it is a good idea to consider keeping a general record of all relevant information and the related processing operations, of which 'personal data' represent just one aspect.

Make sure that, once these insights into information management have been obtained, they are retained. Make the retention of these insights part of the organisation's change management processes.

Risk-aware behaviour

Every employee must be aware of their contribution to and shared responsibility for the careful management of information. This applies to IT managers in particular. Working with information must go hand in hand with clear instructions regarding what is and is not permitted. In the case of important or sensitive information, training courses and/or periodical awareness campaigns could be considered.

How do you identify and manage risks?

Once you have identified and managed your information, you can work on identifying and managing the risks associated with that information. Here too, a number of different steps will be involved.

Role of the board

The board is ultimately responsible for what happens within the organisation. In the event of a serious information-related incident the impact of which extends beyond the organisation, the board will be held accountable by regulators, the media, stakeholders and/or other interested parties.

Ownership of risks

Since incidents involving important or sensitive information can affect the entire organisation, ensuring that information is managed safely and with due care is the responsibility of the board. The board can delegate responsibility for this on a day-to-day basis to the information owners. In order to ensure that risks are managed effectively, the board will require information owners to report on the fulfilment of their responsibility and will make changes where necessary.

Chief Information Security Officer

The management of risks, particularly those associated with digital information, requires specific expertise. Consequently, to allow them to fulfil their responsibilities in this regard effectively, the information owners must be supported by an expert.

A Chief Information Security Officer (CISO) can help with this. A CISO has the following three main roles:

- advice: answering questions on information security within the organisation;
- coordination: responsibility for specific actions in the field of information security, such as, for example, management of the ISMS, supervision of risk analyses, penetration tests or awareness campaigns and keeping a record of security incidents; and
- auditing: checking that the organisation is compliant with the information security regulations adopted by the board and keeping the board informed in this regard.

Although the CISO is often positioned within the IT department in practice, this is not the ideal place, because it can lead to a conflict of interests with the IT manager. Just like information management, the CISO must have an autonomous, independent position within the organisation, which provides direct access to the board and line management. The CISO must be able to report freely without the

person who is responsible for the subject matter of the report standing in the way.

An IT department that needs an employee who focuses specifically on IT security can employ an IT security officer who works closely with the CISO.

Identifying and managing risks

ISO 31000 explains how to set up and implement risk management, and ISO 27005 explains how to do so for information security specifically. In addition to a number of general and essential matters, both standards describe the following steps, which can be used to identify, analyse, evaluate and manage risks.

1. Risk analysis

Risks can be identified and analysed using a risk analysis. Risk analyses can be approached in many different ways, ranging from a pragmatic workshop to detailed methodologies. None of these approaches is right or wrong. The best approach is an approach that meets the needs of the organisation and that the organisation is comfortable with. Ultimately, however, it is advisable to adopt a consistent approach across the entire organisation, so the results of different risk analyses can be compared with each other and progress over time can be measured.

Responsibility for identifying strategic risks lies with the board and responsibility for identifying tactical and operational risks lies with the information owners. The CISO can facilitate and support these processes but can never be the process owner or implement this process without the board or the information owner. A CISO who initiates risk analyses independently may find it difficult to get the relevant owner to accept the risks that have been identified.

A risk analysis must be well prepared. The facilitator of such an analysis must be familiar with the chosen approach and those present must be fully aware of what will happen and what is expected of them. A session must at least be attended by the information owner, plus the necessary domain experts.

A risk analysis may determine that a risk is acceptable and can therefore be accepted. Make sure the risk analysis is attended by someone who is authorised to accept risks.

It is essential also to understand the risks associated with corporate information that is in the hands of external parties. You should ensure therefore that this is included in your risk analysis. Make someone within your organisation responsible for this external processing. Define the assurance required regarding the security of the information held by this external party based on the sensitivity of the information. In the case of low-sensitivity data, confidence in the external party may be sufficient. Where data is more sensitive, a statement from the board may be advisable. If information is highly sensitive, certification, e.g. ISO 27001 or ISAE3402, may be required. Make sure the scope of this certification is adequate.

2. Selection of measures

Where the identified risks are not or not fully accepted, measures to counter them will be selected. The CISO can offer advice or support in this regard. Some risk analysis tools offer automated selection of measures based on predefined risks. You are advised to review this selection carefully and to consider measures other than those contained in the tool.

We assess risks on the basis of probability × impact. The probability is determined by everything that contributes to the occurrence of an incident and the impact includes all the consequences of an incident. Measures can focus on reducing probability, impact or both, so make sure the impact of the measures is in line with the desired approach to a risk.

To reduce the risk of shadow IT, make sure the measures are agreed with the affected user group. Discuss measures that could conflict in some way or to some extent with

the corporate objectives with people who have the authority to make a decision in this regard.

3. Implementation of the measures

Some risk-reducing measures will have to be implemented by other departments, often the IT department. A measure may therefore have a different owner than the risk it is intended to address. Consequently, proper agreements must be drawn up regarding implementation and management of the measures by a different department and regarding the making of changes to the measures.

If an organisation does not work with internal cost allocation, the costs of the security measures that must be implemented will be payable by the department that implements them. This may mean that an information owner is less critical when selecting a measure, which may lead to more measures than are necessary and, as a result, to unnecessarily higher costs. A less critical information owner may also be less involved with the implementation of the measure, which may have a negative impact on the effectiveness of this measure.

4. Monitoring of progress and feedback

It must be checked that measures have been properly implemented and that the intended effect remains for as long as it is required. This is not the job of the CISO. It is the responsibility of the information owner. Progress with the implementation of measures implemented by third parties is therefore reported directly to the information owner.

The CISO reports independently to the board on progress with implementation. Wherever possible, these reports will be included in existing risk and other reports, so information security is not seen as something separate.

Information Security Management System

In order to ensure that the entire process, from identification of risks to reporting to the board, as described in the previous sections, is properly embedded in the organisation, an Information Security Management System (ISMS) can be set up, as described in ISO 27001.

Collaboration

For information and the risks associated with it to be managed effectively, there must be effective collaboration between everyone involved in the process. In addition to the information owner, information manager, CISO and IT manager mentioned previously, this also includes the data protection officer and/or privacy officer. Where necessary, in order to ensure that information is managed in a uniform and consistent way, queries and requests for assistance from information owners will be dealt with jointly by the parties involved. This is something that the board must strive for.

Publication
National Cyber Security Centre (NCSC)
Postbox 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

july 2020