

Why Information Risk is a Board-level Issue

- Every organisation, regardless of its sector, handles information. This information must be appropriately controlled and protected against the threats, non-technical as well as technical, that can affect it.
- Compromised information can cause enormous damage to an organisation's operations and reputation. Information not appropriately protected can lead to serious compliance and legal failures.
- Good Information Risk Management helps an organisation get the best out of its information and allows it to move forward and develop, confident that its risks are under control.

What is Information Risk?

Information, in whatever form, is a valuable asset to any organisation. It is the basis on which strategic decisions are made and daily tasks are performed. Executives, staff, customers and stakeholders all rely on that information being accurate and complete.

There are many ways that good information can be undermined. Corrupted or compromised information can cause a wide range of problems, from those that are simply annoying to those that could have a major impact on an organisation's future.

Information Risk encompasses all the challenges that result from an organisation's need to control and protect its information.

Why Information Risk is an Important Issue

The value of information as an asset extends beyond its volume. Where it is the basis on which executives, customers and investors make critical decisions, it is essential for that information to be accurate and complete. An organisation's success depends on the trust and goodwill of staff, suppliers, customers, and the public at large, so it is essential that all its information is properly managed, controlled and protected.

Why it is a Board-level Issue

Because of the magnitude of the damage that can be caused. Poorly managed information can lead to a material impact on an organisation's future. Because information risks can affect an organisation in every way: financially operationally, they can damage reputation, they can lead to regulatory sanctions.

Because how an organisation addresses information risk will need to reflect ever changing demands and the complex dynamics of the business environment. Strategic direction is required. And finally because directors have accountability in law for how their organisation protects its information. Only the directors collectively have the necessary vision, organisational understanding, and authority required to address this issue.

Should All Information Risks be Mitigated?

Information risk has potentially critical consequences and it should be approached in much the same way as any other critical area of risk.

The key is to determine the level of risk faced by your organisation, and the level of risk the Board is prepared to tolerate.

Gauging the impact if a significant risk were realised is essential. How harmful would it be if, somewhere within your organisation, critical information were:

- Used improperly by staff to facilitate fraud?
- Not available to those who need it when they need it, or not known to be available by those intended to benefit from it?
- Inaccurate or incorrect?
- Lost or disclosed to competitors or the media?

Understanding your organisation's ability to tolerate risk is also important. How much would progress be impaired, interrupted or blown off course if:

- A member of staff was found to have abused the private information of a customer?

- A product was poorly designed and a customer suffered harm in some way
- Data and analysis you had been building up over the past ten months was stolen, by person or persons unknown?
- Your organisation developed a reputation, unfairly or otherwise, for losing sensitive information?
- Current information in a database used every day got overwritten by a month-old back-up?

If you allow your organisation to carry too much information risk:

- You could be forced to apply expensive tactical solutions to a problem that could have been addressed more efficiently with foresight.
- You could be forced to apologise to your customer base or to provide undertakings to the ICO.
- Your organisation could become the example everyone else uses to justify their internal risk management investments.

If the consequences of information risks materialising would be more than the Board is prepared to accept, then you need to take steps to mitigate the risks. The purpose of information risk management is to reduce your organisation's information risks to an acceptable level and to keep them under control in a manageable way, rather than try to eliminate them entirely.

