

Identifying & Managing IT Risks to Your Business

In a competitive business environment, every organization operates in a climate of risk. It is never possible to remove all risk from a business, but it is important to assess and reduce risk to an acceptable level where possible.

In relation to IT, assessing and minimizing risk has recently become very important, particularly for businesses that rely heavily on technology. Therefore, it's vital that business owners understand, monitor, and control risk - especially as the IT environment changes rapidly and new IT-related risks appear regularly.

This guide will help you to identify and assess the IT-related risks facing your business. It will also give ideas on how to reduce these risks and their potential impact.

Examples of IT-related risks

Business managers are accustomed to recognizing commercial threats and taking appropriate actions - for example, dealing with a new customer who turns out to be a late payer.

However, IT-related threats in business are much newer, a lot less predictable and change much faster.

A useful way of recognizing threats is to classify them as follows:

- **Physical threats** are those that result from physical access or damage to information resources such as servers, network equipment, computer rooms, etc. In some business environments, it is easy to overlook these types of threats. However, if an unauthorized person - employee or not - can enter your computer room unobserved, then all your other IT security measures are essentially compromised.
- **Electronic threats** are those that aim to compromise your business information and typically come from outside your premises/network, e.g. a hacker accessing your network via your website. Other malicious threats can range from phishing and spoofing emails and websites to links in social networking websites that take you to websites that can steal your personal and financial details. Hackers can gain remote control of your computers through infections by viruses, worms, or Trojans, turning them into 'bots' or 'zombie computers'. These groups of infected machines - botnets - are capable of a wide variety of activities, including denial-of-service attacks, click fraud, and identity theft.
- **Technical failure** is a common threat for IT systems. For example, if key data were stored only on the hard disk of one server, then the failure of that hard disk would be catastrophic. Hard disks in computers will fail eventually, even in expensive servers.
- **Infrastructure failure** can be a subtle form of threat. For example, if your business relies on your internet connection to receive orders from customers, you could miss out on new purchase orders if that connection fails.
- **Human error** is a major threat. If an honest mistake by a user or system manager could cause an irrevocable loss of data, you need to take action to prevent it from happening, e.g. by regularly backing up data.

Risk management procedure

Risk management should be seen as an ongoing process, rather than a one-off procedure that you apply to an individual threat. You should continuously reassess threats and actively search for new ones.

Risk management is a structured way of controlling risk. There are various ways you can do this, but the following steps outline a typical approach:

- **Identify risk** - to manage risk, you have to be able to identify potential threats. This allows you to act before something happens, rather than 'fire-fighting' after an event. For more information, see the page in this guide on [identifying risk](#).
- **Risk assessment** - you might not need to invest time and money in reducing risk, but you need to take a measured approach to it. Assess its importance to your business. If the risk is serious enough, then you may need to take further action. Some risks may not warrant further work.
- **Risk mitigation - risk reduction** - with many risks you can implement preventative measures that will significantly reduce the probability of the risk occurring.
- **Risk mitigation - impact reduction** - for some risks, you may not be able to reduce the probability of them occurring to an acceptable level. Therefore, you should think more about reducing the negative consequences of that risk should it actually affect your business.
- **Contingency planning** - often the best you can do is make plans for how you would survive a problem. Contingency plans are what you would do after the worst has happened. A particularly important form of contingency plan is a disaster recovery plan. See our guide on [business continuity planning in IT](#).

Identifying risk

To manage IT risks effectively you have to be able to identify potential threats. In the fast-moving world of IT, this can be difficult. However, you can take some effective preventative measures.

A good starting point for identifying risk is hiring a consulting firm, such as [IntegrIT Network Solutions](#), to perform a [Site Vulnerability Assessment](#).

Another technique that can help you to identify threats is a **what-if analysis**. This works better in a small group using a **brainstorming approach**.

Start with simple questions and scenarios to see if they can help to identify new risks. For example, ask questions such as 'what if the telephone line to the building got cut by a digger?', or 'what if the same happened to our power?', and see what plans you need or already have in place to cope with these eventualities.

Another important step in identifying risks is to write them down in a **risk register** as you assess them, so you have a permanent record. You can record in the register what you do about each risk as well as the probability of the risk occurring and use it as a checklist when you review your risks periodically.

Risk assessment

Care should be taken when assessing the risks your business may face. You do not want to spend time and money avoiding or reducing those risks that pose little or no threat to your business.

Once you have identified the risks that do pose a threat to your business, it may be helpful to base your risk assessment on the following factors:

- the **probability** or **likelihood** of each risk materializing
- the **cost** or **impact** of the problem if it did happen

A **quantitative assessment** of your risks would be the numerical product of these two factors. For example, if a risk has a high probability and a high cost/impact, then it will get a high-risk assessment.

Unfortunately, quantitative measures of risk like this are only meaningful when you have good data. You may not have the necessary historical data to work out probability, and cost estimates on IT-related risks change so quickly that accurate financial data is rarely available.

Therefore, a more practical approach is to use a **qualitative assessment**. In this case, you use your judgment to decide whether the probability of occurrence is high, medium, or low. You do this similarly for cost/impact. You might then take action on risks that are high probability/medium cost, medium/high, or high/high, and leave the rest.

Define what you would consider to be low, medium, and high cost to your business in whatever terms seem useful, for example:

- **low** - would lose up to half an hour of production
- **medium** - would cause complete shutdown for at least three days
- **high** - would cause irrevocable loss to the business

Use the same principles for probability. For example, you might classify as 'high probability' something that you expect to happen several times a year. You might classify as 'low probability' something that you expect to happen very infrequently.

Risk mitigation - risk reduction

If your assessment shows that you have unacceptably high levels of risks to your business, then you need to take some action to counter them.

You could:

- reduce the probability of the risk affecting your business
- limit the impact of the risk if it does occur

In practice, you will often wish to do both. However, generally you should try to reduce the probability of the risk affecting your business in the first place.

One way of doing this is **risk avoidance**, i.e. avoiding doing the things that could lead to a problem occurring, such as not entering into a line of business, a particular deal or a new IT project, because it carries a risk.

However, this might mean that you end up not doing anything new, and hence not being able to benefit fully from business opportunities.

You could instead take a more positive approach by changing the way in which you carry out an activity. This is quite appropriate to IT-related risk, and usually involves adopting a best practice approach to acquiring or operating IT systems.

Risk mitigation - impact reduction

There are inevitably some risks to your business that you can neither eliminate nor reduce to an acceptable level.

For these, you can only mitigate those risks by assessing what might happen as a result of the problem and reducing their impact should they occur.

In many situations, the greatest damage can occur because no one fully understands the nature of the problem and end up making it worse.

This can be avoided by common-sense procedures, which should be part of your risk mitigation approach:

- Do not take any actions that could **exacerbate the problem**. For example, if there is a problem with accessing files from a back-up tape using a tape drive, you should investigate whether the problem is caused by the drive, rather than just assuming there is a problem with the tape and then potentially damaging other tapes by placing them in a faulty drive.
- **Implement document procedures** for dealing with likely threats, and train your staff in their use. For example, there are many ways that a virus can get into your system, so you should have plans for quarantining affected parts of the system so that the problem doesn't spread.

An important part of impact reduction is the **early detection of problems**. Where you have a risk that you can't eliminate, you should ensure that you have a fail-safe method of detecting the problem if it occurs.

Often failures are very obvious. However, occasionally, particularly in continuous or recurring processes, a failure may occur silently, and its impact will grow over time. If you identify this type of risk, you should build in a periodic check to detect the problem as soon as possible.

Don't forget that, to reduce the cost impact of a problem should it occur, you could take out insurance. This is a form of **risk transfer** and is a normal part of doing business.

Sometimes you can write risk transfer clauses into the contracts for a deal such as a project. IT risk is, however, difficult or very costly to transfer effectively. Hiring a consulting firm, such as **IntegrIT Network Solutions**, to guide you through this process will ensure a proper assessment.

Practical actions for business managers

Risk management is relatively straightforward if you follow some basic principles. Below are some practical hints that you may find useful.

- Actively look for IT-related risks that could impact your business. If possible, use a small team to identify possible risks. A workshop environment will help you to think more imaginatively about risks than working alone.
- Assess IT-related risks using either a **quantitative or qualitative approach**. This will allow you to concentrate on those risks that are really important and not waste time on those that are not. How you actually measure the risk is less important than the activity itself, which aims to help you review risks rationally.
- Don't produce contingency plans for every risk you identify. This is a waste of time and effort. Concentrate on those problems that would have a serious impact, and where you cannot reduce the probability of them happening to an acceptable level.
- You need a **business continuity plan** (BCP) to cover any serious IT-related risks that could jeopardize your business and which you cannot fully control. If you don't have a BCP, you should work on this first. See the page in this guide on **contingency plans**.
- **Risk management is a continuous process**. If you have not updated your risk register for a while, then there are likely to be new IT-related risks that you have not covered. Similarly, if you haven't looked at or tested your BCP for a while, it may have become out of date. Therefore, you may need to review these as soon as possible.
- Even very small businesses need to review IT-related risks. The time taken need only be small, but it gives important assurance.

Contingency plans

A contingency plan is an impact-reduction measure. It should describe in detail what you and your staff will do if a particular problem occurs.

You may need a contingency plan when:

- you **identify** a risk that you think has a high chance of happening and will have a high impact
- you try to find ways of **reducing** the likelihood of the event, but you cannot reduce the risk to an acceptable level
- the residual risk is still so large that you need to take a **structured approach** to reduce its likely impact

The **main considerations** that you should address in a contingency plan are:

- **scope** - what particular risk the contingency plan is designed for
- **initiation** - how you will know when to put the plan into action
- **actions** - what sequence of actions you will take in order to control the problem and minimize its impact
- **roles and responsibilities** - who will do what and when



Good contingency plans are usually based on the shared experience of managers working together.

An important form of contingency plan is a **business continuity plan** (BCP). This is typically created to cover the most serious of problems, such as the complete loss of all your servers and network infrastructure due to a fire.

Such plans may involve planning for the rapid acquisition of temporary buildings, reciprocal arrangements with other organizations, special staffing arrangements, etc. See our guide on **crisis management and business continuity planning**.

BCPs should be **tested** if possible. A test could be a simple paper exercise where different parts of the recovery procedure are run through by the people involved. This is adequate for simple plans.

A full test of a BCP requires a full exercise. This will usually involve many people and significant cost because it will disrupt normal activities. Therefore, any exercise of this type should be carefully planned and budgeted.