HOW TO MANAGE TECHNOLOGY RISK IN A SMALL OR MEDIUM-SIZED BUSINESS

advance

HOW TO MANAGE TECHNOLOGY RISK IN A SMALL OR MEDIUM-SIZED BUSINESS

Risk is an inherent part of everything we do in life and in business. From crossing the road in the morning to investing in a new business venture, everything involves some level of risk.

But as businesses move from the micro size (1-5 employees) through to small (5-25) and medium (25-200) size, risk management is one element that is often overlooked.

While actively identifying and treating risk may not be a priority in the start-up stages of business, no business can successfully scale without effective risk management strategies.

Put simply, the proactive management of risks can save vast amounts of money when compared with the costs of reactively responding to risks after they have turned into operational issues.

This whitepaper focuses on managing technology and cybersecurity risks; however, the principles can be applied across all risk types within a business.

WHAT IS RISK MANAGEMENT?

The various methods used to minimise and resolve threats to an organisation's profits, proprietary information, and other sensitive assets are referred to as risk management.

The fact that SMEs often overlook or deprioritise risk management is even more surprising given that this can lead not only to increased operational costs but, in many cases, to serious security breaches and data loss.

IT risk management encompasses a wide variety of issues, which are only expanding as businesses rely more and more on cloud services and data storage.

These include information security risk, which relates to how data is handled and managed across the business; cybersecurity risk, which relates to the controls and protections placed around systems; and technology risk, which relates to the performance and operational cost of the IT environment.

WHY IS RISK MANAGEMENT IMPORTANT IN IT?

For an SME, proper management of information and cybersecurity is essential to smooth and efficient operations.

The global IT landscape is changing faster than ever before, meaning businesses can find or lose competitive advantages almost overnight, and cyber threat actors are constantly finding new ways to exploit and profit from businesses that do not manage their cybersecurity risk effectively.

For a business, operating without risk management is akin to crossing the road without looking both ways. Without understanding and planning for the types of risk they face, businesses will find themselves simply moving from one crisis to the next, expending cash and resources on fixes that never should have been needed.

Risk management, particularly in information technology, is not simply about removing risk, but about reducing it to a manageable level and accepting the level of risk that the business is comfortable with.

ELEMENTS OF GOOD RISK MANAGEMENT

RISK IDENTIFICATION

The most important factor in risk management is identifying risk. This involves logging all of the potential issues a business may face. When management moves away from operating blind and becomes aware of the relevant dangers, its decision-making can change for the better.

Although identifying general business risks is often best handled by management, more specialist areas, such as technology and cybersecurity risk, should usually be placed in the hands of an expert in those fields. This may be a specialist provider engaged to perform a more in-depth risk assessment.

Alternatively, if the business has already partnered with another organisation to support and deliver IT, that partner may be best suited to perform risk identification within their area of expertise—especially if the business no longer has the relevant skills in-house.

However, although responsibility for risk identification may be delegated to various parties, management still remains accountable for ensuring risks all types of risks are being identified.

A particularly effective strategy for ensuring robust risk identification is in place within IT is to ensure an appropriate person or organisation is responsible for identifying risks that fall into each of the three risk types.

TYPES OF INFORMATION TECHNOLOGY RISK

Information technology experts typically break IT risk into three main types: Operational technology risk, cybersecurity risk and information security risk.

OPERATIONAL TECHNOLOGY RISK

Operational technology risk involves threats to the business's IT environment, usually from the standpoint of operational efficiency, cost or supportability. Managing this type of risk management means ensuring that the IT a business uses meets its availability requirements and supports an efficient workforce.

It may also look at the cost of technology upgrades and the accompanying risk of change vs. the cost of continuing to support older technology and the risk of disruptions impacting productivity.

CYBERSECURITY RISK

Almost everything done in cybersecurity is about risk management. Unlike other areas of IT, investment in cybersecurity rarely results in direct increases in revenue or profit.
However, just as with physical security tools like locks and CCTV, cybersecurity investment protects a business from unexpected loss. Cybersecurity looks at the technical controls and protections placed around systems and equipment, seeking to ensure that the risk of cyber incidents is reduced to a level in line with the business's risk profile and acceptable tolerances.

Cybersecurity risk management may look at new types of threats and ensure the business's current defences are effective against them, or it may examine how the business's operation has changed recently and the new systems it uses, ensuring they are reasonably protected against attacks.

INFORMATION SECURITY RISK

Information security has a much broader reach than other IT risks, as it spans how data and information are managed across an entire business. Information security focuses more on the business's people and process elements to maintain the confidentiality, availability, and integrity of data.

As a result, managing this type of risk may involve areas such as employee contracts, ensuring data confidentiality is stipulated, or that appropriate authority and approvals are included in processes that manage data access and permissions.

PRIORITISATION AND OWNERSHIP OF RISK

As each risk is discovered, it must be prioritised. This is usually done by assessing the likelihood of a negative outcome and the impact such an outcome would have on the business. Once the priority of a risk is understood, the businesses can then compare the costs and benefits of various treatment options.

Ownership of risk remediation must also be assigned to ensure accountability for its progress. Businesses may assign ownership based on function or on priority, with higher levels of seniority owning higher-priority risks.

A simple risk prioritisation calculation can be found below:

Risk Likelihood		**Risk Impact**	
Likelihood of risk occurring within a 12-month period		Impact to the business if the risk does occur	
Score	Definition	Score	Definition
1	0% - 20% chance of occurring	1	Minor impact to internal productivity, <$1,000 to fix, no impact to reputation, no impact to future revenue
2	21% - 40% chance of occurring	2	Some impact to internal productivity, <$5,000 to fix, no impact to reputation, no impact to future revenue
3	41% - 60% chance of occurring	3	Impact to internal productivity, <$10,000 to fix, may impact business reputation and/or future revenue
4	61% - 80% chance of occurring	4	Large to internal productivity, <$20,000 to fix, will impact business reputation and/or future revenue
5	81% - 100% chance of occurring	5	Major impact to internal productivity, >$20,000 to fix, will significantly impact business reputation and/or future revenue

Risk priority = likelihood score multiplied by impact score

TREATMENT AND RESPONSE

Once a risk has been identified and prioritised, the business must decide how best to handle it.

The four primary IT risk response techniques are as follows.

- **AVOIDANCE:**

  Taking actions to ensure the risk never occurs. Examples include avoiding the risk of old hardware failing by moving to a cloud-based service or avoiding the risk of data theft by completely deleting a data repository. Completely avoiding risks is not often possible.

- **MITIGATION:**

  Reducing the likelihood or impact of a risk to an acceptable level. Examples of mitigation include introducing vendor support contracts to mitigate the cost and duration of system outages or introducing next-generation anti-virus software to mitigate the risk of ransomware.

- **TRANSFER:**

  Passing on risks to another party through commercial arrangements. For example, the risk of costly cyber recovery activities may be transferred to an IT provider through an outsourcing contract or to an insurance provider through an insurance policy.

- **ACCEPTANCE:**

  Agreeing that the business is comfortable with the risk, based on its likelihood, impact and cost of other treatment options. Some risks may be too small for a business to worry about, and others may be too costly to mitigate or transfer. In these scenarios, a business can choose to take no action and accept the risk for a period of time. Accepted risks should be reviewed on a regular basis to determine whether new, more cost-effective treatment options are available or whether the likelihood/impact has increased, and the risk now warrants a different response.

FIRST-TIME RISK MANAGEMENT FOR SMES

Many small and medium businesses operate without risk management, which is risky in itself. However, implementing basic risk management doesn't need to be costly or time-consuming.

The most basic form of risk management doesn't involve expensive tooling or dedicated resources; all it takes is a simple log of risks and activities (risk register) and regular reviews with management support. Many businesses begin their risk management work with a simple spreadsheet and monthly meetings.

Risk management can be implemented first for a specific area that stands to benefit the most, such as information technology or for a specific project. Initially, businesses can focus on the highest-priority risks, with the scope of risk management expanding over time to encompass more risk and/or more business functions as leaders and staff become more confident with risk management processes.

The most important element for initiating risk management is managerial support. Without strong support from business leaders, risk management is rarely effective, risks are often left untreated, or treatment quickly stalls. Partners can also be valuable in initiating risk management as they can identify risks in their area of expertise and recommend potential treatment options.

Like every aspect of running a business, risk management is best started with a straightforward and efficient process. Once it becomes a habit, the process can be matured and expanded until it meets the needs of the business without becoming overcomplicated or overly time-consuming.

CONCLUSION

Risk mitigation through business continuity and disaster recovery planning is critical for all businesses. The length to which disasters are planned and simulated may vary based on the business size. Still, even small businesses should have a basic plan to respond to various possible disaster situations. In today's world, outages and data breaches caused by cybercriminals and other cybersecurity issues must be included in an effective disaster recovery or business continuity plan.

Contact Info

+61 8 8238 6500

sales@advance.net.au

www.advance.net.au