offsite servers

GUIDE TO TECHNOLOGY RISK

CERTIFICATED REGISTERED FIRM
QUALITY REGISTERED FIRM
ISO 9001:2015
QSL
ISO QUALITY SERVICES LTD.
BS EN ISO
ISO QUALITY SERVICES
QUALITY MANAGEMENT

CERTIFICATED REGISTERED FIRM
QUALITY REGISTERED FIRM
ISO 27001:2013
QSL
ISO QUALITY SERVICES LTD.
BS EN ISO
ISO QUALITY SERVICES
INFORMATION SECURITY MANAGEMENT

IT Risk Managment and Managing the Risk

Information technology (IT) plays a critical role in a businesses.

It is important to identify risks to your IT systems and data, to reduce or manage those risks, and to develop a response plan in the event of an IT crisis. Business owners have legal obligations in relation to privacy, electronic transactions, and staff training that influence IT risk management strategies.

IT risks include hardware and software failure, human error, spam, viruses and malicious attacks, as well as disasters such as fires, cyclones or floods.

You can manage IT risks by completing a business risk assessment. Having a business continuity plan can help your business recover from an IT incident with minimal downtime.

This guide helps you understand the IT risks. Offsite Servers can help you manage the risks and expectations of a failure to the business.

Managing the Risk

Managing information technology (IT) risks is a structured process that involves a series of activities designed to:

- Identify
- Assess
- Mitigate
- Develop response plans
- Review procedures

Business continuity planning

Having identified risks and likely business impacts, the development of a business continuity plan can help your business survive and recover from an IT crisis. A business continuity plan identifies critical business activities, risks, response plans and recovery procedures.

IT risk management policies & procedures

IT policies and procedures explain to staff, contractors and customers the importance of managing IT risks and may form part of your risk management and business continuity plans.

IT risk assessment

An effective IT risk assessment identifies serious risks, based on the probability that the risk will occur, and the costs of business impacts and recovery.

Security policies and procedures can assist your staff training on issues such as:

- Safe email use
- Setting out processes for common tasks
- Managing changes to IT systems
- Responses to IT incidents

A code of conduct can provide staff and customers with clear direction and define acceptable behaviours in relation to key IT issues, such as protection of privacy and ethical conduct.

The Risks in IT...

Your business relies on information technology (IT) systems such as computers and networks for key business activities you need to be aware of the range and nature of risks to those systems.

General IT threats

General threats to IT systems and data include:

- **Hardware and software failure** - such as power loss or data corruption
- **Malware** - malicious software designed to disrupt computer operation
- **Viruses** - computer code that can copy itself and spread from one computer to another, often disrupting computer operations
- **Spam, scams and phishing** - unsolicited email that seeks to fool people into revealing personal details or buying fraudulent goods
- **Human error** - incorrect data processing, careless data disposal, or accidental opening of infected email attachments.

Criminal IT threats

Specific or targeted criminal threats to IT systems and data include:

- **Hackers** - people who illegally break into computer systems
- **Fraud** - using a computer to alter data for illegal benefit
- **Password theft** - often a target for malicious hackers
- **Denial-of-service** - online attacks that prevent website access for authorised users
- **Security breaches** - includes physical break-ins as well as online intrusion
- **Staff dishonesty** - theft of relevant data or sensitive information, such as customer details

Natural disasters and IT

Natural disasters such as storms and floods also present risks to IT systems, data and infrastructure. Damage to buildings and computer hardware can result in loss or corruption of data.

Reduce the Risk

Threats and risks to information technology (IT) systems and data are an everyday reality for any modern business. Measures should be put in place to protect your systems and data against theft and hackers.

Practical steps to improve IT security

- Secure computers, servers and wireless networks
- Use quality anti-virus and anti-spyware protection, and firewalls
- Regularly update software and operating systems to the latest versions
- Use a recognised data backup that includes offsite or remote storage
- Secure your passwords (ask us about password security)
- Train your staff in IT policies and procedures
- Understand legal obligations for data protection and loss of client data protocols

Create a secure online presence

Secure socket layer (SSL) technology is used to encrypt transaction data to send customers card details to the acquiring bank for authorisation. You should ensure any web hosting solution you consider is capable of supporting the SSL protocol.

Induction and IT training for staff

Training new and existing staff in your IT policies, procedures and codes of conduct is an important component of IT risk management strategies. Training can cover key business processes and policies, such as:

- safe handling of infected email
- protecting the privacy of client data
- priority actions in the event of an online security breach

As an employer you have legal obligations when training staff. Providing support and training for new employees is a critical aspect of staff training.

Business insurance

It is impossible for a business to prevent or avoid all IT risks and threats. This makes business insurance an essential part of IT risk management and recovery planning. You should regularly review and update your insurance, especially in light of new or emerging IT risks, such as the increasing use of personal mobile devices for workplace activities.

Responding to an IT incident

How you respond to information technology (IT) incidents determines how well your business recovers, and also influences customers' ideas about your reliability.

An IT incident can be confined to the IT components of your business, such as a denial of service attack that targets your business. An IT incident can also be part of a wider business crisis, such as widespread damage to networks due to natural disasters.

Your IT risk management plan and business continuity plan should include:

- IT incident response plans
- Emergency response plans
- Recovery plans

IT incident response plans

IT incident response plans identify principal risks and the steps you need to take to mitigate effects or damage. They may include details of key staff who need to be notified, priority actions, communication plans, contact lists and an event log to record actions taken.

Emergency response plans

IT incidents may be the result of a wider crisis, such as an explosion, storm or flood. An IT incident response plan should integrate with and support emergency response plans.

IT incident recovery plans

Will help you respond effectively if an IT incident or crisis affects your business. A recovery plan can shorten recovery times and minimise losses, and should include:

- Strategies to recover your businesses activities in the quickest possible time
- Description of key resources, equipment and staff required to recover your operations
- Your recovery time objectives

The conclusion

Whatever IT system you have, whether it is on-premise or hosted offsite (Cloud based) you have risk of losing your data.

How you manage that risk is up to you... Do you rely on your loyal IT staff to do their job who may just run if a 'real' problem occurs? Do you have a an outsourced IT department who assure that its all working correctly because and you only find out when it fails that this isnt the case.

We are a company who can perform an honest risk assement for you so you can brief your staff or outsourced IT company.

The easy option is to do nothing about busines risk and your IT system. Are you prepared for when it all fails?

Offsite Servers Limited - Innovation Centre, 1 Devon Way, Longbridge Technology Park, Birmingham B31 2TS
Telephone 020 33 55 9558 or 0121 272 2030 - www.offsiteservers.com - hello@offsiteservers.com