.Dott
Risk

Managing Your Risk Guide

Technology

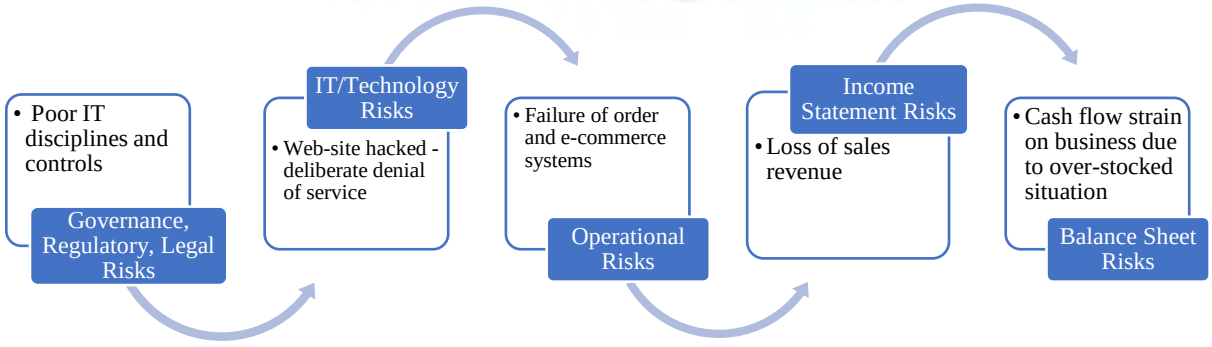
What is this risk area?

IT and technology risks are those that can have a material impact on the operations and financial position of an organisation as a result of a direct or indirect loss arising from failure of systems, networks, loss of data/ information, security breaches, operational system failure, equipment theft, fraud and cybercrime

Where does this risk area emanate from?

This risk arises from the extent of use of technology and IT in the operations of the organisation and the failure, abuse of the required technology or systems. These risks can arise from HR/People, crime, operations, regulatory and physical risks.

Example of IT/Technology risk interconnectedness with other risk areas:



Where does this risk area manifest itself?

This risk can manifest in operational failure, crime, inability to deliver strategy, reputational damage e.g. loss of data, financial losses, balance sheet stress and organisational failure.

Why is it important to manage these risks?

IT and technology risk issues can have a major impact on the operations, reputation and financial position of an organisation. These impacts can be immediate and significant or happen over a period of time but will have a lasting effect on the organisation.

Where to start managing this risk area?

IT and technology risk management starts with a review of the level of IT governance, policies, controls and disciplines throughout the organisation and the effectiveness of these. The review needs to cover and identify gaps and weaknesses in the physical technology environment and potential threats. This includes staff education, user behavior, network and hosting risks, data security and controls, cybercrime risks, service providers, IT resources, back-up and support, firewall controls, anti-virus and related software controls.

What is the benefit of actively managing this risk area?

The management of IT and technology risk will ensure that the organisation is better equipped to prevent and deal with system failure, data loss and theft, fraud, cybercrime and criminal incidents or situations such as sabotage or blackmail in a structured and effective way.

DottRisk has the following detailed risk guides covering what we believe are the critical areas of IT and Technology risk:

Introduction to IT and Technology Risk

Every organisation has an IT/Technology threat profile based upon their business model, the industry they operate in, the type of assets they control or manage, nature of connectivity, their geography and the vulnerability of their IT and technology systems.

Technology risk is ironically ultimately best managed by people.

This means that a culture of awareness and discipline from ALL people is required in order to manage the risks emanating from technology. You also need to clearly define what is expected of staff to help your organisation mitigate the massive increase of technology risk. On-going risk education and awareness training are essential.

The role of network, firewall and security software in eliminating many other technology risks (e.g. data theft, hacking, ransomware, ecommerce fraud) is a basic requirement for the managing of these risks.

Given the integral role which technology and IT plays in every sphere of an organisation's operations, this key area demands good governance – processes and procedures, policies, disciplines, controls and risk mitigation, particularly in the areas of cybercrime, business continuity and disaster recovery.

Legacy operating systems and proprietary software present specific areas of risk. Not only are you continually at risk of not getting system and software support due to skills availability, but the ability to retain compatibility with operating systems and other software remains. The extent to which an organisation uses proprietary software can have a material bearing on the IT risks it faces. These include access to source code, the need for specific control procedures when developing new code or updates, the ability and cost to support and maintain legacy systems and programmes, continuity, security challenges, ability to integrate with other systems and version control being just some of the risk issues which arise here.

Technology and IT are complex and evolving environments, and risk controls therefore have to be on-going too. The role technology and IT play and the dependency upon them varies for each organisation, irrespective of size. The reliance on technology and IT needs to be assessed by each organisation so that the impact of a potential failure or loss arising from these areas can be assessed and quantified.

The level of controls and security required will be dictated by:

- The volume, sensitivity, importance and "value" of your data
- The complexity of your operational environment
- Extent of proprietary software and legacy systems being used
- Nature of your operations
- Extent of mission critical systems
- Reliance on call centre and associated technology
- Potential threats to your organisation and its assets

- Your physical environment
- The number of users
- The extent of access to your systems (web/email/log-ins/device and network connections)
- The extent of home/remote office connectivity
- Regulatory and compliance requirements

The growing threat and risks of cybercrime and security breaches are set to change the face of business. Cybercrime is generally defined as any form of criminal activity involving the use of computers and the Internet. This can arise from both external and internal sources. Attacks can also be malicious and a form of sabotage. As technology and risk evolve, this will necessitate a global, forward-looking, and layered security response to protect your organisation from new and as yet inconceivable threats. Cybercrime poses such a significant risk to the operations of larger organisations that it is now recommended as a key reportable board item.

Hackers do not only focus on government or large organisations but launch cyber-attacks on all sorts of businesses and entities. This includes hospitals, police operations, non-profit organisations and universities – in fact any entity they can possibly get to co-operate and pay a ransom.

IT and technology security cannot be an afterthought and need to be engineered to ensure secure and trustworthy computing. With the arrival of technologies such as robotics, synthetic biology, artificial intelligence, blockchain and nanotechnologies, there will be far more disruption in future.

One of the biggest threats facing any organisation is the loss of data and systems. A balance has to be achieved between the availability and security of data within an organisation. The integrity of data and maintenance of information confidentiality is also of paramount importance.

The contagion effect of technology risk or the knock-on effect of these risks should never be overlooked or be under-estimated. Most risks manifest themselves in other risks. Technology and IT risks whether arising from a criminal activity such as hacking or a physical event such as a natural disaster or failure in the normal course of operations, can quickly impact and manifest in operational, financial, reputation and legal risks.

In addition to data controls, the control of system access, password controls, physical security of IT systems and the protection from power surges and other un-anticipated events all need to be managed and safeguarded. File, file sharing, mobile, mail and gateway security controls are all essential.

There are hundreds of millions of malicious targeted and untargeted e-mail phishing and spam attacks daily, so in addition to anti-virus and encryption controls, firewall and secure message management and e-mail security are needed to ensure safe system access and business continuity. Data breach investigations have shown that even with training, a high percentage of phishing emails are still opened by staff, so protecting the organisation against human error is a top priority. The same goes for the accessing of unprotected web-sites.

Systems availability and accessibility 24/7 is now a basic business requirement for both the staff and customers of most organisations. System outages and down-time in an organisation has a material impact on productivity, organisational processes and controls, security controls, service levels, business enquiries and sales. Given the erratic state of electricity supply in many locations, it is imperative that organisations have back-up power supply/generators/UPS or inverter devices in place in order to reduce these risks. The use of outsourced data centres (as opposed to in-sourced centres) has enabled many organisations to mitigate the risks of power outages and a lack of system back-up capacity.

The use of cloud and virtual back-up sites and data centres has also lowered the risk of loss of data and the costs of running or making use of expensive off-site disaster recovery sites. Having guaranteed access to the source code material for mission critical systems is also essential.

An area that has a big impact on network availability, systems performance and user internet access in an organisation is that of line stability/reliability, bandwidth availability, line speed and data storage capacity. Given that bandwidth is effectively a scarce commodity, it has to be managed to enable optimum availability and accessibility for business use. In order to manage bandwidth usage, firewall shaping has to be pro-actively managed. This can involve restricting access to particular internet sites, limiting e-mail downloads and restricting bandwidth available for accessing social networks, you-tube and drop box. It is also possible and advisable to load internet restrictions on all laptops and mobile devices that are given access to the organisation's network.

The digital revolution has changed the way business is being done, but at the same time has created a complex set of security and risk issues. Assets that were once physically protected are now accessible, customer channels are reachable and opportunities for theft and fraud are constantly increasing. With most businesses needing to be "on" or "connected" at all times, this has materially increased the risk of attack. The simplest of devices can now facilitate access and with opportunity, comes risk requiring an increasing risk management focus. The inability of an organisation to control its data or security can have an immediate result in a loss of confidence and business.

At the same time users/customers have to feel comfortable when interacting with on-line systems.

The steps to be taken to reduce these risks need to focus on the following key distinct areas:

- IT and Technology Governance – Processes and Procedures, Training and Awareness
- Web-site security
- End Point Protection – Patch management programmes, Data protection, Anti-virus Software, Firewalls, Physical assets, Remote working protection
- Network security
- Operational Controls – including System Monitoring, Penetration/Ethical hacking testing
- Incident Tracking
- E-commerce and Banking Controls

- Regulatory and Compliance
- HR/People Controls and associated Criminality
- Cyber Security and Cyber Liability Insurance Cover
- Disaster Recovery
- Project Management

IT and Technology Governance – Processes and Procedures, Core Measures, Advanced Measures, Bring Your Own Device (BYOD)/Working Remotely

The governance of the IT and technology areas require the same level of oversight and disciplines as are present and exercised in other key areas of the organisation such as finance, HR and operations.

The extent of processes and controls will be dictated by the by the sensitivity and "value" of your data, complexity of the operational environment, extent of proprietary software being used, nature of your operations, potential threats, your physical environment, number of users, the extent of access to your systems (web-site/email activity/log-ins/e-commerce/ device and network connections/remote connectivity) and the regulatory environment.

Any organisation that allows or encourages the use of personal devices for work purposes should ensure that a "Bring Your Own Device" ("**BYOD**") policy is in place.

When it comes to the security of devices and with that, ensuring information security, organisations should, at the very minimum, impose strict rules to ensure that such devices are password protected (in this regard, a password policy is strongly recommended) and should require that anti-virus software be installed thereon.

E-commerce and Banking Controls

E-commerce and Banking Controls have been identified to be the most vulnerable/prone to internal (staff and employees) abuse and external (outsiders) attacks. As a result of this, it is advised that organisations deploy very strict disciplines and controls. The key ones being strong password controls and segregation of duties among operators. An organisation becomes highly vulnerable to its website being hacked and its customer transaction information (bank accounts and/or credit card details) being compromised if tight e-commerce security controls and disciplines are not deployed.

General and specific controls should be deployed to best manage and mitigate these risks.

Cyber Security

Technology is ever changing and requires constant awareness of cybercrime activity and vulnerability. Small and medium (SME) companies are more vulnerable than large companies to cybercrime because they do not have large budgets for IT security and do not have dedicated resources within the company to manage the risk. Hackers are now targeting businesses of all sizes - looking for data to exploit, holding businesses to ransom and performing financial transactions by diverting monies into their own bank accounts. Some attacks are performed by staff or ex staff members and are malicious. These can manifest in on-line vandalism, sabotage or blackmail.

Ransom attacks invariably see organisations and in turn their customers, "locked out" of their own systems where access is encrypted with the attackers demanding payment, often in the form of untraceable bitcoin, for the release of the encryption keys. Each organisation needs to have a response to such attacks and how they plan to deal with the threat and potential loss of data and the loss of customer access.

Existing and potential clients of service organisations want to be sure they are engaging with an organisation that takes cyber security seriously, including addressing the cyber security risks inherent in the outsourcing of certain functions to a third party.

End Point Protection – Data, Software, Physical Assets, Firewalls, Network and Home/Remote office working controls

Endpoint protection refers to a system for network security management that focuses on network endpoints, or individual devices such as workstations and mobile devices from which a network is accessed. The term also describes specific software packages that address endpoint security.

The complexity, extent, number of users and degree of access to your systems and network determine the level of risk an organisation may be exposed to. The massive increase in "home /remote office connectivity" and video link ups has further increased the need for added focus on security controls.

You need to determine what endpoint protection you will require for home/remote users and put appropriate controls in place. E.g. ensuring that remote access doesn't introduce more risks, ensuring that VPN solutions are up to date, use of geo-blocking, enhanced remote working policies and Covid-19 scam education.

IT and Technology HR/People Controls

Employees are singularly the biggest risk to an organisation so it is imperative that all the necessary background screening and reference checks are performed before employees are placed in positions of trust, deal with critical systems and sensitive data. Disciplines around IT/technology staff are also integral in managing the risk of criminality in these areas.

As organisation leaders have you educated and made all your IT, finance, bookkeeping, credit, operations and accounting staff etc. fully aware of the various cyber-crime, banking scams, control circumvention and fraudulent and criminal activities being perpetrated and attempted by fraudsters and syndicates.

Operational Controls, Incident Tracking, Regulatory and Compliance, Disaster Recovery

With technology and IT playing an integral and ever increasingly dominant role in the operations of organisations, rigid operational controls and disciplined processes and procedures need to be put in place to minimise the associated risk. In tandem with this, increased regulatory compliance is required, notably around data confidentiality. Added security controls are required across a broad spectrum from technical to cybercrime and physical. All security incidents need to be tracked, investigated and closed. Given the reliance on technology and IT, these areas need to form key parts of business continuity and disaster recovery plans.

Given the potential impact, all IT and technology incidents should be taken seriously, be recorded and be formally responded to and dealt with.

Given the increasing use of technology, connected devices, digital and social media, the regulatory and compliance environment becomes more complex and ever evolving.

Organisations must manage, govern and ensure compliance for the overwhelming amount of data they produce and/or are entrusted with by customers, especially in the face of global legislation rather than just complying with national regulations.

You need to have a disaster recovery or business continuity plan in place to counter criminal acts and natural disasters that are likely to severely disrupt the operations and sustainability of your organisation, e.g. fire, floods, theft of equipment, loss of data, sabotage, ransoms, acts of violence, riots, destruction of property, cable theft or loss of fibre/telecom links.

IT and Technology Project Risk

IT and technology projects such as the implementation of new systems, critical systems rewrites, new operating systems, web-site rewrites, upgrading networks, telecom systems or security/access control systems are common in most small/medium sized businesses. These require the same project management disciplines as for any traditional construction or installation project to ensure that the risks associated are minimised and managed.

Web-Site Security

Websites have become an integral part of most businesses, with an ever-increasing percentage of business being done on-line. You need to be continually checking on the on-going effectiveness of your site from a content, security and functionality perspective. You need to make use of displays, flash features, mobile displays and optimise search engine criteria by using key and ad words. Hacking of websites is now commonplace so security here is essential to enable business continuity.