



## IT Systems. Compliant or just complex?

*by Sean Lynch, Partner*

Not too long ago, IT systems were viewed as tools to support the core functions of a business. Now IT systems are at the very core of most businesses, and are critical in determining the success or failure of a business.

The scope and importance of IT systems for most businesses has moved far beyond the desktop computer. The convergence of the technology and telecommunications sectors is producing new products and services faster than users can keep up with. Businesses are transferring and processing different types of data between different devices over different and complex networks. Most businesses now have to consider a range of mobile devices linking to their IT systems, whether to outsource some or all of their IT systems operation and maintenance, and whether to utilise new technologies to automate various aspects of the business.

The impact of IT systems within businesses has also moved far beyond the IT Department. Sales, Operations, HR and even the Board of Directors is affected as apart from IT systems now being the heart, mind and nervous system of the day to day operation of most businesses, they play a critical part in ensuring that your business fulfils its legal compliance obligations. Your IT systems should be ensuring proper governance and best practice for your business.

At present, many Boards either do not recognise these compliance related risks as being associated with their IT systems, or if they do, will just delegate all issues to their IT managers and expect them to cover these sorts of risks off. This is where the potential for disconnect and future failure can occur. The IT Department is not equipped to be the sole assessor of end to end compliance and best practice.

Breaching legal obligations relating to someone else's data or intellectual property can have dire consequences for your brand, reputation and share price – not to mention the actual costs involved with addressing the breach. There have been many high profile incidents reported in the media in recent years.

### **Compliance – some examples**

Legal compliance requirements and risks relating to the use of IT systems include:

- Privacy laws – constraints on the receipt, storage and use of personal information.
- Spam – you need to know what the compliance requirements actually mean for your business in terms of consents required, evidence, storage etc... and how your IT systems (say a new CRM system) can best assist with meeting these requirements and marketing to your customers and prospects.
- Confidential Information – ensuring that your systems and users are not breaching confidential information rights held by a third party.
- Intellectual Property – ensuring that your systems and users are not breaching the intellectual property rights held by a third party, and that your business has all the required rights to use and disclose all intellectual property used.

- Your contracts – are there any specific provisions in your contracts with third parties that need to be addressed within your IT systems? Do your IT contracts ‘do their best’ to ensure that your company will meet all of its compliance obligations?
- Your employees – are your IT systems up to date and configured to comply with the current employment laws?
- Industry or sector specific laws – are there laws which are specific to your business or industry sector which an “off the shelf” IT system (often purchased from an offshore vendor) does not consider or address? Does targeted legislation such as the Public Records Act apply to your organisation? Does your business need to comply with specific resource management or emissions compliance requirements and therefore have a need to capture and store certain information?
- Litigation & Evidence – you need to ensure that your IT systems retain the best evidence possible of your compliance with all required laws, stored in a manner which is readily accessible and confirms the high integrity of that data.
- Money Laundering – is your business impacted by the current laws or proposed reforms in this area? Are your IT systems designed to reduce this risk?
- Defamation – does your business operate a blog on its website? Is it monitored and moderated to ensure that third party rights are not breached?

The above are a few compliance issues to consider. There may be others.

### **What you need to do**

These issues need to be considered and effectively addressed at the right time, and regular audits and updates carried out. Broadly the process should look something like this:

1. Before any major IT systems upgrade or acquisition occurs, engage a good commercial / IT lawyer and have that person meet with your risk manager(s) and IT people to review specific contract issues and comprehensively examine wider compliance issues;
2. Prepare a compliance identification and action report, assess to what extent the new IT system should address or help mitigate these risks, and build this into the functional specification;
3. Ensure that your IT contracts with your suppliers address and effectively cover all required compliance issues (with teeth);
4. Some issues relate not so much to the IT system itself but rather to the content inputted or used within the system. It is prudent to develop systems and processes for the delivery and / or storage of certain types of content to ensure that compliance is achieved and that highly sensitive data is stored and transferred in the most secure manner possible.

Failure to take these steps before committing to a costly upgrade may result in risk and cost later on for your business which far outweighs the cost of taking these steps at the outset.

**For further information contact Sean Lynch on 375 8722 or [sean.lynch@heskethenry.co.nz](mailto:sean.lynch@heskethenry.co.nz)**

