

The Recession, Information Security and You.

Discover five ways to protect yourself!

We're all aware the world is in deep recession, and companies and public sector organisations of all sizes are tightening their belts.

The fallout effects - such as loss of earnings, confidence and even jobs - can seem even worse when morale is low. Most significant is the heightened risk of a break-down in the disciplines that keep a company going, and a key area of importance will be the handling and management of corporate information.

It's widely acknowledged that employees with low job security have a more vested interest in their own welfare than the security of corporate information. Worse still, it may even occur to them that this information has a value. So where does the responsibility really lie?

Weathering the Storm

Survival is the name of the game, and whilst this statement may sound bleak, never has the need to look after 'number one' been more prevalent or more acceptable. Recession tends to nurture a culture of 'every man for himself!'

So, with redundancies, reduced working hours and cash flow pressures to contend with, what do we actually mean by 'number one'? Ultimately, it's the company, and that also means it's principle asset; it's people.

This is the time for the Board to consider morale, motivation and communications processes within their organisations. When morale is low, maintaining policy and procedure becomes harder. It's a small step for a breakdown of policy to result in the loss of person identifiable information, data or even product-related intellectual property to a competitor. The loss or scandal could just be enough to tip the balance between surviving, and not.

It's not about Information Technology!

Information-Security is not just about Information Technology; it never has been. First and foremost it is directly and unequivocally linked to the people it touches day to day. These are your people, and your asset. With the recession taking hold, it is important to encourage positive morale and general motivation.

Corporate governance must consider any risks to a company's assets, which may impact upon its ability to function. With regards to staff, the answer is simple communicate well and maintain as positive morale as possible.

The 5 Key points to consider.

1. Identify a healthy balance between revenue generation and regulatory compliance. Information-Security should not hamper revenue generation, but revenue should not be threatened as a result of poor information and data-handling.
2. If your business handles person identifiable information, find out if it should be registered with the Information Commissioner's Office.
3. Do not rely upon Information Technology! Take positive steps to help the users and remember, it's the company's responsibility to offer adequate training. The knowledge-gap between I.T. and users is increasing, so never assume that users understand their responsibilities, or the implications of flouting them. A simple lack of understanding or education could lead to an expensive security breach.
4. Many users are hesitant to discuss information security because they feel it's a 'technical' subject, or one that doesn't really affect them. Overcome this challenge by presenting the subject positively, reiterating the value that individuals place on their **own** privacy. Do they assume that their own data is safe? Wouldn't they want a business holding **their** information to take the appropriate steps to protect it? Delivered this way, and perhaps in bite-sized chunks, the topics can be made relevant and interesting - and as such is more likely to be effectively retained.
5. Display posters and/or other printed material around the building, with simple messages such as '**remember to lock your workstation**' or "**pick-up print runs**" etc. Keep them simple and not patronising.

Particularly when the economy at large is under pressure, businesses need to protect themselves and minimise risk wherever possible. With lost laptops and discs being made huge examples of by the media, it's not a time to gloss over the very real implications of a security loss. It starts and ends with the people who utilise the data, and educating them is a great way to protect your business.

Nigel Landman

Chairman, QT&C Group