The role of insurance in mitigating compliance risks

Every company in the world that provides business-to-business services is now having to consider risk and compliance management, says **Paul Norris** of Reason Global Insurance

Data security is an important part of compliance and the international moving business is particularly vulnerable to breaches because personal information – such as passport copies and national insurance numbers – is exchanged as a necessary part of the process. If the worst happens, does your company insurance provide any protection

CONTINUES OVER

FOTOGESTOEBER / SHUTTERSTOCK

FOTOGESTOEBER / SHUTTERSTOCK

to you, your customers or their assignees? If it doesn't, it should.

The general term 'compliance' includes the requirement for companies to: operate within regional regulations, such as the UK Bribery Act of 2010 and the US Foreign Corrupt Policies Act; comply with all contractual obligations; and behave in a way that develops trust between the company and its customers. What's more, it also requires companies to take responsibility for the whole supply chain. It's a tough challenge – many say an impossible one – and even the most vigilant company lives in fear of a breach that can prove devastating for themselves and their customers.

Data security, too, is an important part of compliance, with companies being required to ensure that all personal information held on behalf of clients, is kept safe. However, with the level of cyber attacks increasing, the chances of a company being hit are significant. If a breach occurs, the costs – direct and indirect – can be crippling. New EU regulations in 2016 will require businesses to comply with more onerous rules concerning notification to the Information Commissioner's Office, explicit consent to hold and process data, and the right to be forgotten. Breaches could result in significant fines of up to two per cent of a company's turnover.

A report by the UK government and risk consultants Marsh – *UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk* (March 2015) – estimates that 81 per cent of large UK companies, and 60 per cent of small businesses, suffered a cyber-security breach in 2014. Officials also estimate the cost to small and medium sized (SME) businesses in the UK from the theft of customer data at £1bn.

A survey by PricewaterhouseCoopers, carried out in 2012, found that 72 per cent of small businesses reported staff misuse of email or the internet, and the unauthorised access of files resulting in a Data Protection Act breach, or misuse or leakage of confidential information.

This is not just a problem for the moving company concerned. A high proportion of international relocations are performed on behalf of employees of multinational companies, and are controlled through relocation management companies (RMCs). These large customers rely, absolutely, on their reputations and any small slip will be exploited by a controversy-hungry media. Similarly, the RMCs need to demonstrate to their clients that they deal harshly with compliance transgressors. A data-protection breach would easily be enough to lose a moving company its contract with a major corporation, which will take a 'zero tolerance' approach.

Insurance cover cannot prevent a breach, but it could just keep a mover in business should a breach occur. It might even give a corporate client some comfort that the mover takes the whole compliance issue seriously and, therefore, become a powerful part of the sales proposition.

APPROPRIATE COVER

It's fair to say, however, that cyber-risks insurance is an emerging market and many policies do not include it. So it makes sense for movers to work with their brokers to develop cover that is appropriate for their individual businesses. For example, cover for: system damage; business interruption; theft of money; cyber extortion; reputational damage; and claims by third parties – possibly the client or the RMC – after a security breach. These could include the cost of meeting claims for the loss of confidential data under the Data Protection Act and regulatory investigations caused by hacking.

If a breach occurs, the response from the insurance company will be to provide a range of services to protect the business and minimise the detrimental effects. These can include: the employment of public relations, crisis management, forensic and speciality services; financial compensation; the cost of replacing equipment and recovering information; business-interruption costs; fines imposed by government or the public authority regulator; costs of notifying the data protection authorities of the breach; and the payment of extortion fees with associated negotiation, handling, contracting and delivery of monies.

If a corporate client has a 'zero tolerance' policy, any data breach is likely to result in a serious penalty or loss of the contract for the mover. That is bad enough, but there's no need for it to bring down the company. Appropriate insurance can help a business to ride the storm – and help protect customers too. FF

HOW TO KEEP YOUR IT SYSTEM SAFE

1. Ensure your network and firewalls are relevant and secure enough
2. Make it mandatory that passwords have to be changed regularly
3. Set up your staff user accounts for the levels of access they need. No more than that
4. Ensure that your anti-virus and malware programmes are up to date and maintained
5. Encrypt mobile devices, such as laptops, if they carry sensitive data away from the workplace network

More tips and details on cyber security can be found within this article from international law firm Taylor Wessing: **http://united-kingdom.taylorwessing.com/globaldatahub/article_cyber_security_tips.html**