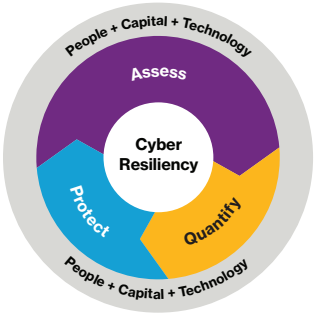


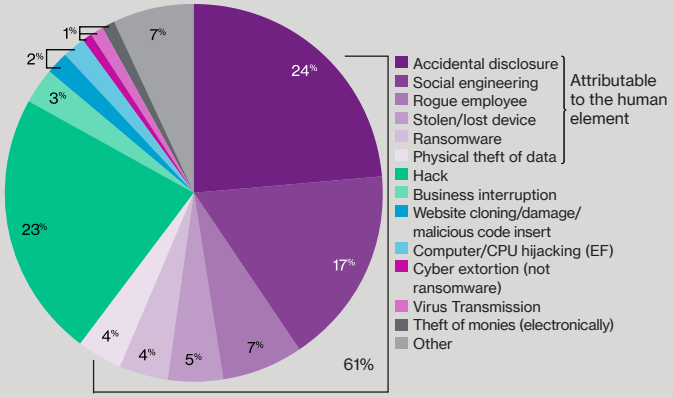
Decode people risk.

Court rulings leave UK companies financially exposed to data protection misdeeds of rogue employees

By Andrew Hill, Willis Towers Watson

In a recent claim involving the deliberate disclosure of personal data belonging to 100,000 of UK supermarket Morrisons' employees by a rogue employee, a senior IT auditor at the organization, the High Court held that, whilst Morrisons was not directly liable for the data breach (i.e. it was not at fault), it was vicariously liable for the rogue employee who caused the data breach.

Type of Loss



Source: Willis Towers Watson 2017-18 Reported Cyber Claims Index

7% of the claims within the Willis Towers Watson 2017-18 Reported Cyber Claims Index involved rogue employees. The Morrisons decision increases the potential exposure resulting from these types of incidents beyond the costs associated with incident response. By allowing the recovery of substantial damages against employers of rogue employees on a theory of vicarious liability, more plaintiffs will be enticed to file such lawsuits

Although Morrisons appealed the decision, on 22 October 2018, the Court of Appeal upheld the High Court's decision, notwithstanding:

1. Morrisons had taken all reasonable steps to prevent the misuse; and
2. It was the employee's intention to cause financial or reputational damage to Morrisons.

The ruling has potentially far-reaching implications for organisations, although it is understood Morrisons intends to appeal the decision in the Supreme Court.

The wider impact for organisations

The scope for significant damages

It was submitted on behalf of Morrisons that, in circumstances where an employer was found to have acted reasonably in preventing the misuse of personal data, a finding of vicarious liability would potentially place an enormous financial burden on innocent employers.

The Court of Appeal accepted that, depending on the facts, data breaches caused by corporate system failures or negligence by individuals acting in the course of their employment might give rise to a significant number of claims against companies for "*potentially ruinous amounts*".

Willis Towers Watson

The potential for more data protection claims

The Court of Appeal's landmark decision would appear to put organisations at greater risk than ever before of being on the receiving end of a data protection class action. Even in circumstances where employers have taken all reasonable steps to prevent the misuse of personal data, it can be extremely difficult to detect and stop a rogue employee. Following the Morrisons decision, employers in the UK are now exposed to being held vicariously liable for the actions of such employees. The decision will not have gone unnoticed by claimants' solicitors who specialise in data protection class actions.

The Court of Appeal says insurance is the solution

Having acknowledged that large scale data breaches may lead to class actions that could be ruinous for employers, the solution, said the Court of Appeal, is to insure against such catastrophes. Although the Court recognised that an organisation should not be automatically imposed with liability just because they purchase insurance, it added that insurance is "*a valid answer to the Doomsday and Armageddon*" concerns raised by Morrisons.

Will Employers' Liability / Public Liability insurance cover data protection claims where the affected data subjects are seeking compensation for non-material damage?

The General Data Protection Regulation (GDPR), which came into effect on 25 May 2018 (i.e. after the events which gave rise to the Morrisons action), gives data subjects an express right to be compensated for non-material damage (e.g. non-financial loss such as distress) for any non-compliance. Even prior to the GDPR, in 2015 (i.e. before the events in Morrisons) the Court of Appeal held in *Google v Vidal-Hall & Ors* [2015] EWCA Civ 311 that individuals are entitled to seek compensation for non-material damage for (1) a breach of the Data Protection Act 1998 (DPA 1998) or (2) any breach of the tort known as 'misuse of private information'.

This evolution of damages in the context of personal data, whether under the DPA 1998, the tort of misuse of private information, or the GDPR, gives rise to the question of how Employers' Liability (for actions by employees) and/or Public Liability (for actions by third parties) insurance, both of which typically cover claims arising out of 'bodily injury', are likely to respond in the event of a data protection class action in which compensation is being sought for distress. The expectation is that Employers' Liability (EL) and Public Liability (PL) policies would, prima facie, provide cover for data protection claims seeking damages for non-financial loss such as anguish or distress, provided the definition of 'bodily injury' in the policy is sufficiently broad. It is important to note, however, that these policies are not designed to cover financial loss. Therefore, in circumstances where a claimant alleges pure financial loss, a typical EL/PL policy would not provide cover.

Given the pace of developments in the sphere of data protection, it is unclear whether it was ever the intention of EL/PL underwriters to cover the potentially significant claims envisaged by the Court of Appeal in Morrisons. Therefore, it remains to be seen what action, if any, EL/PL insurers will take to address the rights individuals now have to claim damages for distress. Equally, organisations may want to consider whether their existing EL and PL policy limits are appropriate in view of the Court of Appeal's comments.

How cyberinsurance cover might respond in a Morrisons-type case

A typical cyberinsurance policy provides cover quite distinct from that found in EL and PL policies. In the event of a data breach, including the one which gave rise to the class action against Morrisons, a cyberinsurance policy is designed to work in two key ways:

1. Indemnify the policyholder for the costs it incurs dealing with and mitigating against the impact of the data breach (first party costs). These typically comprise:
   - IT forensic costs
   - Legal costs
   - Notification costs
   - Credit monitoring for affected individuals
   - Call centre costs
   - Regulatory investigation/proceeding costs

2. To the extent an EL/PL policy (1) does not cover data protection claims alleging pure financial loss and/or (2) sub-limits or even excludes data protection claims seeking damages for distress or anguish, cyberinsurance is designed to indemnify the policyholder for any damages, claimants' costs and defence costs arising from any legal proceedings alleging, by way of example, mental anguish arising from the misuse of personal data or non-compliance with any data protection legislation (third party costs).

What impact does the Court of Appeal's decision regarding vicarious liability have on cyberinsurance policies?

Organisations that already purchase cyberinsurance may ask what, if any, impact the Court of Appeal's decision might have on the coverage available within their policy.

Where a claim is made against the policyholder alleging, for example, misuse of personal data, and, as was the case in Morrisons, if it is a rogue employee who is alleged to have been responsible for that misuse, a standard cyberinsurance policy would cover any damages and costs, notwithstanding any argument the policyholder may have concerning its vicarious liability for the actions of a rogue employee. This is because the relevant cover is triggered when a claim is made against the policyholder (which is usually a defined term in the policy) rather than on the basis of who is alleged to have been responsible (subject to what is said below). Were a court to find that the policyholder is vicariously liable for the actions of a rogue employee and award damages to the claimant(s), it would be expected that the policy would respond in the usual way. If, on the other hand, a court were to find the policyholder is not vicariously liable, the expectation would be that the cyberinsurance policy indemnifies the policyholder for any costs it has to bear.

The Morrisons decision also emphasises the importance of ensuring that an organisation's cyberinsurance policy (or any other applicable liability policy for that matter) provides cover for the acts of all individuals for whom the organisation may be vicariously liable in damages. Equally important, is ensuring careful consideration is given over to several exclusions typically found in cyberinsurance policies which, if not tightly drafted, could result in the exclusion of what would otherwise be a covered claim.

Contact

Andrew Hill
+44 (0)203 124 8278 (ext: 18278)
hillanx@willistowerswatson.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

WTW-NA-2018-WTW163861

willistowerswatson.com

Willis Towers Watson