UK Professions

Protecting through Prevention

WM Morrison supermarkets PLC "landmark" data breach ruling could have implications for businesses across the UK.

A disgruntled employee of the Morrisons supermarket chain posted online the personal information and payroll data of nearly 100,000 staff in 2014; current and former staff took the company to court arguing that the company is responsible for breaches of privacy, confidence and data protection laws, and sought compensation for upset and distress caused.

What has the privacy breach cost?

Morrisons has incurred £2,000,000 in costs as a result of this privacy breach already, with additional legal fees and a potential settlement on the horizon.

A future court hearing will determine what compensation Morrisons must pay to the 5,518 claimants. Any payment would open the door to the other 94,480 individuals affected to also make a claim. The UK Information Commissioner's Office (ICO) does not provide guidelines about levels of compensation in this area. If the parties cannot agree on an appropriate level, the court will have to decide and until such time the company will continue to incur legal fees.

The ICO has authority to charge fines up to £500,000 for serious breaches of the Data Protection Act, however, it seems unlikely that they would fine Morrisons, who were ultimately the victim of criminal activity in this instance.

Why is this news?

Liability arising out of a data breach has been largely viewed as a "US issue" due to tight regulations and a reputation for being highly litigious, especially with respect to class action lawsuits.

The company has incurred remarkable costs considering that the higher cost items seen in other privacy breaches aren't a factor in this case: the breach was not caused by a hacker so there was no network incident to investigate, there was no systems damage to remediate or to disrupt revenue, and the claimants are seeking compensation for upset and distress as opposed to actual financial harm.

The new EU data protection law, General Data Protection Regulation (GDPR) hasn't taken effect yet (25th May 2018)! Discussions about data protection have recently been focused on developing and testing corporate policies and technological safeguards and employee training. But, as we know, no control or set of controls is 100 per cent effective to detect or prevent unwanted employee behaviour, especially when the attacker is an authorised user of information resources.

If this incident had occurred after the implementation of GDPR, Morrisons would have incurred additional costs to notify each of the 100,000 impacted individuals since the breach resulted in a high risk to their individual rights and freedoms.

Paragon

Why is this matter relevant to every UK Company?

The privacy breach was caused by a trusted employee, and while no misuse of private information and breach of confidentiality could be established under the Data Protection Act 1998, it was ruled that the company was held responsible for the actions of that employee.

Based on this decision, one of the first under UK Law, companies could in future expect to receive class action-type lawsuits following a privacy breach.

The Morrisons case highlights the costs that can arise out of a privacy breach even where only vicariously liable and a company could be held vicariously liable for data loss caused by their service providers or through their supply chain. Within the approved judgement, the Honourable Mr Justice Langstaff himself highlighted the relevance of insuring vicarious liability by appropriate insurance.

What is Cyber insurance?

Cyber insurance provides coverage for privacy liability, network security liability and costs involved with recovery after a cyber incident:

- whether caused by a hacker or by an employee,
- whether personal data is exposed in print or electronic format,
- whether the company is directly or vicariously liable.

Most insurance policies are an after thought, providing reimbursement for losses incurred after the insured event is over. Cyber insurance policies are different; they do offer reimbursement but also can take an active role to help businesses recover from a cyber incident as it is happening. A well-constructed cyber insurance policy will often have a panel of experienced vendors to triage a cyber incident which can supplement
or tie into a company's existing business continuity plan (meanwhile supporting GDPR requirements for breach notification).

Summary

Prevention is always better than trying to detect, contain, and recover from an incident, yet the likelihood that companies will experience a privacy breach or a security incident continues to rise. As a result, breach preparedness is an absolute must (even before GDPR). Many cyber insurance policies can assist by providing a panel of breach responders if an incident elevates outside of your internal capabilities, as well as by providing important balance sheet protection.

For more information about cyber insurance, please contact...

JANINE PARKER
Partner and Head of UK Professions
E jparker@paragonbrokers.com
T +44 (0) 20 7280 8207
M 07920 516 303

Dated: December 2017

Paragon