Top tips for employers dealing with cybersecurity issues

21 Apr 2016
By: Sandra M Wallace

Prevention

The most important step a business can take to protect itself is to put measures in place to prevent cybersecurity breaches from occurring in the first place. A number of employee related preventative measures are often overlooked. Employers must ensure that their employees are educated about risks the company faces in respect of cybersecurity, what to do to prevent such risks from materializing and, if they do materialize, what steps to take to mitigate the effects of a breach.

Our top tips for prevention of employee cybersecurity breaches are:

- Have strict confidentiality obligations in all employment contracts in relation to the employer's proprietary information, as well as information belonging to customers or trade partners. Also make use of post-termination restrictive covenants where appropriate to protect information after an employee has left the company;
- Have clear, easily accessible policies in place, such as:
  - An IT security policy, including obligations to protect IT equipment, encryption of data and reporting requirements in the event of a breach;
  - An IT and communication systems policy which includes a clear right to monitor internal IT systems and specify prohibited use of the system;
  - A whistleblowing policy to encourage a culture of "speaking up" internally to avoid employees airing the company's dirty laundry in public;
  - A disciplinary procedure that reflects the seriousness of an employee breaching obligations around confidential information and IT security; and
  - A grievance procedure to allow discontented employees to communicate their concerns formally.
- Educate employees about security policies with training and regular refresher activities, and make sure policies are reviewed and updated regularly;

- Remember that the effectiveness of a policy is only as good as the company's treatment of it: employees won't take their obligations seriously if they don't see their employer doing the same; and
- Have a clear zero-tolerance policy regarding bullying, harassment or intimidation of employees who wish to raise, or have raised, concerns regarding potential breaches.

What to do when there is a breach

In an ideal world, implementation of the preventative steps outlined above will mean that no breach occurs. Unfortunately, breaches may still occur, whether accidentally or intentionally. Here are our top tips on dealing with a breach:

- Ensure the breach is contained at any early stage. If it has happened accidentally, ascertain whether there is a potential risk of further breaches occurring in the same manner, and address these with the relevant employees. If the breach has occurred intentionally, take appropriate disciplinary action. Ensure that employees are reminded of the organisation's policies and procedures in respect of cybersecurity;
- Ensure from the outset of a suspected or actual breach that employees who are required to participate in an investigation are clear on the need for their involvement and the importance of confidentiality during the investigation. Ensure all interviews with employees are documented and, where possible, documents are signed by the employee to confirm the content is correct; and
- Where there is a breach and the individual concerned is suspected of criminal conduct, consider whether police involvement is required and how this will interplay with internal disciplinary procedures.

Each company will differ in its needs and preventative measures. Companies must ensure that, as well as having employee-related measures in place, all other aspects of the company are risk-assessed regularly.

Businesses must recognize threats, identify information they need to safeguard, take measures to achieve effective protection and keep such measures under regular review.

Back to Law à la Mode Issue 19

AUTHORS

Sandra M Wallace
Partner
Birmingham | T: +44 (0)20 7349 0296 [UK Switchboard]
Dublin | T: +353 1 436 5450
sandra.wallace@dlapiper.com