LITIGATION NEWS

CLIFFORD GOULDSON LAWYERS

Cyber attack in your business: legal obligations, options and liability

Cyber attacks are on the rise in Australia, particularly those which target businesses - often with quite sophisticated methods.

Late last year, we gave some practical tips on how to minimise the risk of a breach of your business' cyber security.

In this alert, we set out what a business must and can do legally if its cyber security is compromised.

Mandatory data breach notification

If you are unlucky enough to be successfully targeted by a hacker, you must first assess whether the data breach falls under the *Privacy Act 1988* (Cth). If it does, you must promptly notify individuals at likely risk of serious harm and the Australian Information Commissioner. The notification to the Commissioner must be made within 30 days or as soon as practicable.

Who can I sue?

If you fall victim to a cyber attack, the next step you should consider is reporting the incident to the Australian Cyber Security Centre, which is part of the Commonwealth Attorney-General's Department and shares information with the Australian Federal Police, the Australian Criminal Intelligence Commission, the Australian Security Intelligence Organisation and the Australian Signals Directorate.

Moreover, if you are the victim of an online fraud or scam, you are encouraged to report the incident to the Australian Cybercrime Online Reporting Network (**ACORN**). Any report which is made to the ACORN may be referred to the relevant State's police force for consideration and possible investigation.

Victims of cyber attack are on average unable to access their systems for 25 hours. As you would anticipate, this alone can result in significant business losses.

In an attempt to recoup that loss, it may be possible to start a civil court proceeding against the hacker for trespass to your personal property (i.e. unauthorised access to your data), detinue (withholding possession of your data despite demand for its return) and/or conversion (i.e. using that data contrary to your ownership rights). However, identifying the hacker is likely to present a large practical hurdle.

While there have been no Australian cases against hackers, one US company filed a suit against their 'John Doe' hacker and then successfully applied for a pre-trial discovery order, allowing them greater powers to attempt to determine the hacker's identity.

If you've been hacked, you might also have a potential claim against your Information Technology Service and Support Provider, Software Protection Provider and/or Server Host (**IT Providers**) for:

1. breach of contract if your IT Provider agreed that your system would be protected from cyber risks;

2. negligence if the cyber attack occurred as a result of your IT Provider's failure to meet the standard of care expected of an IT Provider in their shoes; and/or

3. various causes of action under the Australian Consumer Law, such as:

a. breach of the guarantee that any software would be of acceptable quality;

b. breach of the guarantee that any software would be fit for its purpose;

c. breach of the guarantee that any technical service would be completed with due care and skill; and/or

d. breach of the guarantee that any technical service would be fit for a particular purpose.

Claiming insurance

Australia is subject to the most cyber attacks of any nation in the Asia Pacific region, with the number of small businesses affected topping 500,000 in 2017. As the threat of cyber attacks continues to rise, cyber attack insurance is becoming increasingly widespread and can cover your business in a number of surprising ways.

Many traditional business insurance areas (Public and Product Liability, Business Interruption, Professional Indemnity, Management Liability, etc) exclude protection for cyber attacks, rendering specific cyber protection even more important. Cyber liability insurance can cover cyber extortion (e.g. ransomware), business interruption costs and mandatory data breach notification expenses, but may also cover public relations and data recovery costs.

The relative novelty of cyber attacks mean that companies are often caught unaware and without adequate protection, often dissuading them from taking steps to recover loss or indeed letting their clients know about the attack. However, we have found that proactively informing stakeholders of the incursion Clifford Gouldson experienced has only strengthened our relationships with them.

As the targeting of employers is on the rise, we recommend they begin to implement cyber attack management programs in their workplaces to heighten awareness, reduce vulnerability and maximise preparedness should an attack occur. Such employee education might also improve the employer's eligibility to claim on their insurance.

Future director liability?

Legal developments on cyber crime are expanding to meet the challenge head-on and many sources believe that an increased legal focus in the field will eventually filter down from regulators

to company directors.

Just as understanding the totality of their company's financial position is a critical director duty, it is thought that cyber risk management will eventually form an integral part of the legal obligations a director owes their company.

Commentators suggest that enlivening director liability for preventable cyber breaches is a sure-fire way to accelerate cyber security development and increase protection of the ever-expanding sensitive personal data that individuals entrust to companies.

Directors should consider cyber security awareness an important part of their professional development. Such awareness can lead to decreased vulnerability, lower losses from attacks, quicker data recovery and reputational repair, and greater protection from liability.

If you've encountered a hacking event in your business, our Litigation + Dispute Resolution team can help you notify affected individuals and the Australian Information Commissioner, identify who's responsible, the quantum of any claim and advise on your legal options to pursue recovery of any loss.

For more information contact our Litigation + Dispute Resolution Team.

Harrison Humphries, Head of Section

Brian Conrick, Senior Consultant

Oliver Dornbusch, Graduate Law Clerk

Alison Cassidy, Paralegal

Contact Us

Phone 07 4688 2188

www.cglaw.com.au