大成 DENTONS

Cyber breach investigations

As recent headlines are showing us, **cyber incidents pose one of the most significant threats to Australian organisations**. It is more important than ever for **directors and officers** to understand their obligations in relation to cyber security practices and to keep data breach risks, compliance and protections at the forefront of their minds. Knowing the **types of data and personal information** being held by an organisation is critical to avoid investigation by a host of regulators who have remits in relation to cyber security incidents, beyond just the Office of the Australian Information Commissioner (OAIC).

A director or officer's failure to mitigate cyber risks faced by their company falls squarely at the heart of **director duty enforcement actions**, making them potentially liable for failing to prevent a foreseeable breach. Further, any **failure to maintain, update or implement appropriate cyber security practices** could also result in a claim against the directors for a failure to act in the best interests of the company. **Some things to consider about the personal data you hold:**

WHAT DETAILS ARE YOU COLLECTING?

The Privacy Act defines 'personal information' as information about an individual that enables identification of that individual. Consider whether you need to collect more than just a name and phone number or email address.

HOW ARE YOU STORING CUSTOMER AND STAFF INFORMATION?

Consider your IT security systems and how the information you are collecting is being stored. If such information is accessible to all staff or is on a non-secure server, consider upgrades and security measures to better protect the information.

WHAT HAPPENS IF A THIRD PARTY ACCESSES THE INFORMATION?

If information collected by you is accessed or lost (either through inadvertence or mishandling) or is stolen as a result of a cyber-attack, you will need to investigate whether your mandatory reporting obligation arises and whether individuals affected need to be advised.

WHAT CAN I USE THE INFORMATION FOR?

Information held can only be used for the purpose for which it was collected. Consider whether you have in place appropriate processes to destroy information collected that is no longer required or which does not need to be held to meet statutory obligations.

HOW CAN I ENSURE THE INFORMATION IS SECURE?

Speak with your IT provider to ensure the most up to date and secure processes are in place to protect information obtained. In addition, training all staff to be 'cyber ready' and on the look at for potential attacks will be critical, as will having up to date privacy and breach response policies.

WHAT DO MY STAFF NEED TO KNOW?

Through dedicated training, your staff need to know how to identify and be vigilant against email scams and phishing attacks to ensure they do not inadvertently allow access to information you hold. Monitor staff activity and identify early high risk behaviour.

HOW DO I REPORT A SUSPECTED LOSS OF INFORMATION?

Knowing your mandatory reporting obligations under the Privacy Act for when a data breach needs to be notified to the OAIC is critical, including assessing whether any loss of personal information would be considered an "eligible data breach" and when affected individuals need to be contacted directly.

Ben Allen
Partner, Australian head of Dentons Global Compliance and Investigations practice
D +61 2 9035 7257
ben.allen@dentons.com