From the editors…

In this issue, Dudley Kneller and Koula Politis discuss the threats, risks and impacts of a cyber attack on the average Australian business and consider the market for cyber security insurance.

Andrew Jaworksi considers the Government's response to the prevalence of on-line piracy. This includes recent amendments to the Co*pyright Act 1968* that have made it easier for rights holders to block content hosted on foreign websites and the proposed *Copyright Notice Scheme Code 2015* which provides for warnings to be issued to individual consumers who unlawfully downloaded copyright material.

Sylvia Song contrasts the treatment of criminal records in Australia and the United Kingdom to explore the inherent conflict between an individual's right to privacy and the public interest in crime in the community.

Finally, Kevin Chen and Christopher Chiam argue for tougher criminal legislation to deal with cyber bullying. They propose additional regulation to cover social media users who 'like', 'share' or 'comment on' harmful content.

The Editors

Daniel Thompson, Isaac Lin, David Ng and Moses Kakaire

With increasing awareness of cyber security issues there is now a variety of information available which provides organisations with advice on how best to combat the risks of cyber security breach events. There is little information however on whether cyber insurance products should form part of your risk mitigation strategy. This article briefly explores the rise in cyber security breaches before discussing the role cyber insurance products can play in mitigating risks in this area.

2. How do cyber security breaches occur?

Before examining the topic in any detail it is helpful to understand first how such breaches can occur in the first place. There are 3 main ways that cyber security breaches can occur: Firstly, as a result of a criminal and/or malicious attacks (i.e. hacking), secondly, through the negligence or mistakes of employees or contractors, and finally as a result of technology or system failure.[3]

Sometimes the breach can be inadvertent, often occurring by interception of email or other data communications. Equally common is the risk of loss of sensitive information or data caused by insiders such as employees who have security clearance to access network and communications systems.

It is clear that businesses need to consider how to design their systems security and access regimes to minimise the risk of unauthorised access to company data and prevent the occurrence of security breaches – both from "within" and "without".

Being adequately prepared will enable you to be in a better position to respond rapidly to a cyber event, to control and manage the subsequent impact on the business and to effectively manage any brand or reputational fall out. Having a plan in place will ultimately save your business both time and money.

3. What are the real risks?

The most obvious risk to your client's business is the loss of commercially sensitive information such as the loss of trade secrets or disclosure of personal information. Laws relating to breach of confidentiality are well established. The remedies available for breach include taking action to try and compensate for the loss and damage suffered by such breach, although damages are not always an adequate remedy.

It is well known that once confidentiality is lost it cannot be regained so it is important to take necessary preventative measures to properly protect and secure information.

If the Privacy Act 1988 (**Privacy Act**) applies to your organisation, you will need to take into account the risks of a failure to secure data where that failure results in a breach of the Privacy Act. The Privacy Act requires entities to take reasonable steps to protect personal information such as customer details. Significant penalties may apply if you are responsible for a breach of the Privacy Act. These include fines of up to $340,000 for individuals and $1.7 million for corporations as well as the potential for compensation orders to be awarded.

Corporates should be aware that company directors need to be adequately informed of the risks of security breaches involving a breach of directors' duties or other liability under the Corporations Act 2001. Directors should consider the risk of shareholder litigation against the board if there is a risk that the board failed to take reasonable steps to mitigate the risks of cybersecurity breaches. In limited circumstances, directors may be exposed to liability for criminal prosecution.

Another risk area involves security breaches or outages that result in systems crashing and the loss of a business' online presence. If a trading entity's website is down or if employees cannot access the network, the business is at risk of losing the online business generated by traffic