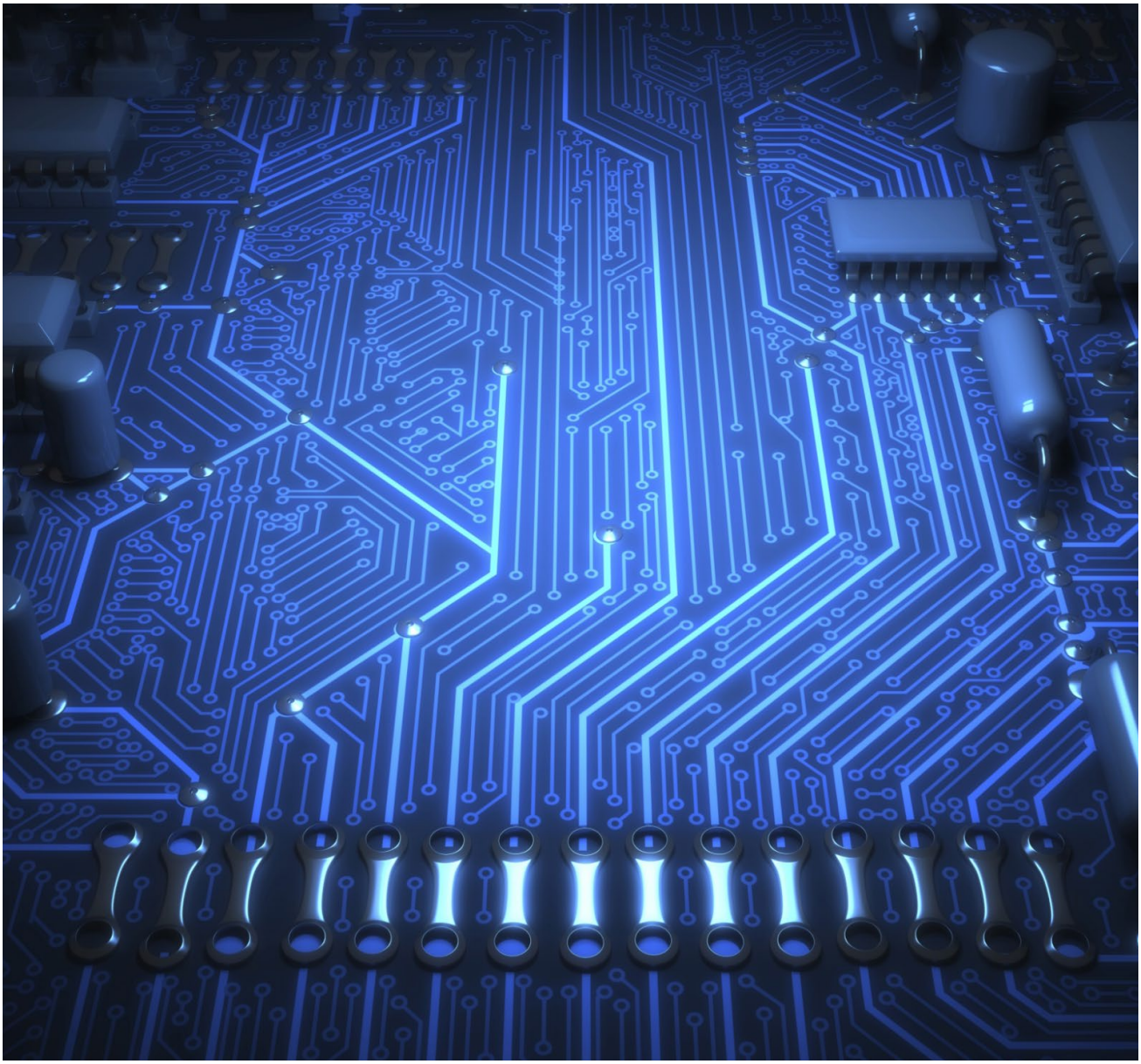
MARSH

DIRECTORS IN THE FIRING LINE: RESPONDING TO CYBER THREATS



INTRODUCTION

It is hard to identify any company that is immune to cyber crime in today's interconnected digital world. First lines of technological defence are no longer impenetrable and directors are now being held directly accountable when the businesses they govern experience a cyber security event.

Data breaches affect millions of records a year: data or network sabotage, virus and Trojan infection, computer fraud and laptop theft, incidents of denial of service and network scanning are ever increasing and it is unlikely the underlying trends will improve. According to the 2014 report from a research center dedicated to privacy, data protection and information security policy, the Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis*, the mean annualised cost of cyber crimes for 257 benchmarked organisations was US$7.6 million per year, with the cost ranging from US$500,000 to US$61 million per company each year. As such, insurance coverage for cyber risks should be a significant and growing concern for companies.

As our research paper, *Cyber Security and the Boardroom Marsh Briefing 2014* shows, some companies that once believed they had little exposure to cyber threats are more than likely to be connected to business partners or customers that are attractive targets and become the entry point of an attack. As a result they can also be at risk from cyber threats.

SPOTLIGHT

Here are some recent examples of the serious consequences to companies stemming from cyber breaches:

2013

In December 2013 hackers accessed the customer records including credit card details of 700,000 Target customers in the US. Subsequently, more than 140 lawsuits have been launched against the company. The business reported US$162 million in expenses across 2013 and 2014 related to its data breach, according to a media release issued on 25 February 2015.

2014

According to a November 24, 2014 filing with the US Securities & Exchange Commission, at least 44 lawsuits were filed against Home Depot by customers, payment card-issuing financial institutions and others in connection with an October 2014 cyber incident.

As such, potential liabilities stemming from cyber security breaches have emerged as a major risk for companies, regardless of size or industry. Consequently, cyber threats are now a key concern for company directors and officers.

Regulators in Australia and abroad have responded by increasing oversight and highlighting the importance of companies making timely disclosures relating to cyber risks. Which makes it more important than ever for directors to understand and discharge their cyber security obligations, especially given they can be personally legally responsible for aspects of the conduct of a company.

Network security and data privacy are no longer the sole province of the IT team. These issues have become a matter of good corporate governance and directors can be answerable to shareholders, customers, business partners and authorities when it comes to these issues.

Some directors and officers are only starting to appreciate the significant personal liability they may be subject to as a consequence of a cyber security breach. As such, this paper explores how directors and officers' (D&O) liability insurance policies can respond to cyber risks.

SPOTLIGHT

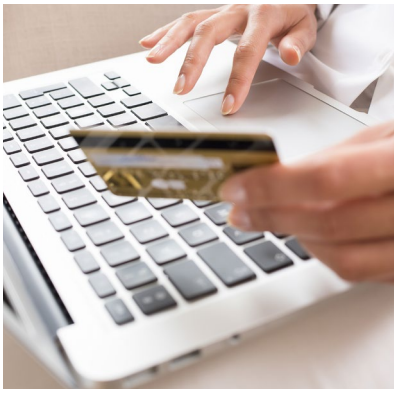
Importantly, boards and management teams, as opposed to technology business units, must be able to answer these three critical questions.

- **WHAT** INFORMATION DOES YOUR COMPANY HOLD?
- **WHERE** IS IT LOCATED?
- **HOW** IS IT PROTECTED?

D&O POLICIES: PERSONAL ASSET PROTECTION

While D&O policies are generally designed to protect directors' personal assets, they may not always respond to cyber risks in the manner expected.

D&O insurance was developed long before the evolution of cyber risks. Consequently, cyber risks may not fit neatly within existing definitions and coverage clauses of a D&O policy, creating possible gaps in cover. It's worth understanding how some D&O policies may respond to a claim as a result of a cyber issue.



D&O POLICY RESPONSE: EXAMINATION OF EXCLUSIONS AND DEFINITIONS

A typical D&O policy may cover individual directors for acts, errors or omissions arising from their conduct as directors subject to the full terms and exclusions. This could include matters relating to a cyber security breach.

Below are some situations that could be covered by some D&O policies:

- Directors not discharging their duty to act with due care and diligence by failing to ensure adequate cyber security measures or failing to purchase and maintain cyber insurance.
- Directors breaching their fiduciary duties for the same reasons and for failing to take appropriate risk mitigation steps to prevent or minimise the impact of a cyber attack.
- Breaching continuous disclosure listing rules.
- Impairment of assets due to incident response costs or payments of regulatory fines or mishandling of crisis management following a cyber incident.
- Directors failing to take reasonable steps to secure customers' personal and financial information.
- Directors failing to provide prompt and adequate notice to affected customers following a cyber breach.
- Directors engaging in misleading and deceptive conduct regarding the consequences of a cyber security breach.
- Shareholder derivative actions brought against boards for failing to exercise proper business judgment in preparing for or dealing with a cyber event.
- Shareholder derivative actions brought against boards for failing to exercise proper business judgment in preparing for or dealing with a cyber event.

on average, the cost of cyber crime per year in US dollars is **$7.6M**

Generally speaking critical definitions such as claim, loss and wrongful acts in many D&O policies are broadly defined so far as coverage for directors and officers is concerned. Therefore, these policies may respond if terms are triggered by a cyber security event.

Further, some D&O insurers now expressly cover cyber risks.

However, aside from an explicit cyber exclusion, other seemingly-unrelated exclusions may also remove potential cyber cover. For example, typical D&O policies often contain a bodily injury and property damage exclusion. Property in this context could include intangible assets such as digital data. Cyber coverage may not apply if this exclusion is couched in broad terms. It's worth noting that in the broader D&O policies this exclusion is limited to damage or destruction to tangible property, leaving the door open for potential claims for damage to intangible property such as data as a result of a cyber security issue.

In addition, some D&O policies specifically exclude cover for fines and penalties. This exclusion will therefore limit any cover a D&O policy may provide following an adverse regulatory finding into a cyber security breach that results in a fine.

The failure to insure, fraud and dishonesty and prior known matters exclusions may also apply, depending on the factual matrix relating to the cyber security breach. The prior known matters exclusion may also give rise to non-disclosures issues because they both deal with matters known by the insured before the policy was incepted.

Further, additional cyber exclusions may be applied in the future as cyber risks are increasingly viewed by insurers as a distinct category of risk, especially in light of evolving new covers that specifically cater for this class of risk.

Exclusions notwithstanding, D&O polices have been called on to respond to cyber security breaches. But directors and officers should be aware their D&O policy may be depleted or even exhausted by a cyber security breach. They should ensure they purchase not only an adequate limit of liability for cyber security insurance but also for their D&O policy in case it becomes a back stop in the event of a claim.

THIRD PARTY VERSES FIRST PARTY COVER

D&O policies principally cover directors and officers for third party losses; that is losses sustained by a third party such as customer, client or supplier as a result of a director's wrongful acts, errors or omissions.

In a D&O policy loss is typically defined to include damages (including compensation orders), judgments (including pre and post judgment interest), settlements entered into with the insurer's consent and defence costs and other associated expenses such as claimant's costs and crisis costs.

We know cyber security breaches also result in a number of first party losses, being direct losses sustained by the company. Damage to property consisting of intangible assets namely software (programs) and data, business interruption, lost market value and remediation and notification expenses are some of the losses sustained directly by a company as a consequence of a cyber security breach. These items are not typically covered by a D&O policy. Consideration should be given to whether directors and officers should mitigate these risks through other insurance policies such as a specific cyber insurance.

REGULATORY INVESTIGATIONS

There is increasing regulatory pressure on companies in relation to their duties and obligations associated with network security and data protection. For instance, the Office of the Australian Information Commissioner (OAIC) has the power to levy fines of up to $1.8 million for companies that are found to have breached privacy laws and fines of up to $360,000 for individuals for breaches of privacy laws. The Australian Securities and Investments Commission (ASIC) and the Australian Prudential Regulation Authority (APRA) are also actively involved in this issue, as are other regulators worldwide. So it's anticipated regulatory investigations arising from a cyber breach will rise.

Regulatory investigations are often serious matters and can result in severe outcomes for directors. Most

FIGURE 1 FINE LEVYS
Office of the Australian Information Commissioner

D&O policies include some form of cover for legal costs incurred by directors or officers in preparing for, responding to and attending an investigation.

The broader D&O policies provide this cover to the full policy limit and apply even when a wrongful act, error or omission has not been alleged (which is important as at least at preliminary stages this may not be clear) and contain an advance payment promise.

The consequences of regulatory breaches can include:

- Criminal prosecutions against the company and its directors and officers.
- Fines and penalties against the company and its directors and officers.
- Director disqualification or imprisonment.
- Follow on civil proceedings.
- Significant legal costs and expenses.
- Damage to reputation and brand.
- Disruption to business.

If a regulator commences a criminal prosecution following an investigation, this can trigger the definition of claim under a typical D&O policy. As a result directors and officers are typically covered for amounts for which they become legally liable in defending such a prosecution.

Cover can also be available for any civil penalty proceedings that may be instigated by a regulator against a director for statutory breaches following an investigation.

Most D&O policies will provide some form of cover for legal costs and expenses incurred by directors in defending disqualification orders.

The broader D&O policies will also cover:

- Reasonable legal costs incurred by a director or officer to bring legal proceedings (as distinct from defending proceedings) to overturn orders disqualifying a director or officer from managing a corporation.
- Reasonable costs and charges in hiring a public relations firm to mitigate the effects of any published negative statements arising out of any investigation and flow on litigation.
- Fines and penalties to the extent insurable at law.
- Associated appeals.

Typically cover for prosecutions against a company itself is not expressly covered.

PRE-INVESTIGATIONS

Cover for pre-investigations is a recent but rapid evolution in the insurance arena, with some D&O policies now providing cover for costs incurred by directors in preparing formal notifications to any regulator or official body of an actual or suspected material breach of a company's legal duty or for conducting any internal investigations where requested by a regulator following a company's formal notification. Cover can be sub-limited and additional premium and conditions may apply. Nevertheless these provisions may be of value in the cyber space. Some insurers are also offering express cover for shareholder derivative suits.

It will be interesting to see how these new covers will be used to respond to future cyber security breaches.

IMPORTANCE OF NOTIFICATION

Given D&O policies may respond to a cyber security breach it's important to take care with reporting of claims and circumstances in relation to any cyber security incident.

It is especially important companies follow the notification and claims handling conditions in the policy so as to not prejudice cover

CYBER RISKS: THE FUTURE

Cyber risks without a doubt present new and different challenges for directors and their companies. They can expose companies and their directors and officers to class action lawsuits, significant recovery costs and can lead to irreversible damage to the corporate and personal brand.

Undoubtedly, the liabilities will continue to grow and evolve as new perils arise.

With so much at stake a thorough understanding of the risks involved and how best they can be managed is paramount. This imperative is echoed by regulators.

It is important directors put procedures in place, including to:

- Identify cyber risks.
- Qualify and rank them.
- Assess controls and countermeasures in place.
- Identify risk improvement procedures.
- Repeat the process regularly and monitor progress.

Once cyber risks are identified, an insurance wording gap analysis can be performed and decisions made to negotiate extensions to current wordings or place a specific cyber policy to either supplement existing policies or act as a first line of defence.

While a D&O policy may provide some relief in respect of the liabilities and losses flowing from a cyber security breach it may not always respond in the manner expected.

New cyber specific insurance policies are emerging to fill the gaps and should be carefully considered by companies and their directors and officers.

These policies can be specifically designed to cover a range of cyber risks including both first party losses and third party liabilities as well as to afford cover for associated legal expenses, settlements, judgments, regulatory investigations and other related business expenses, for example, privacy notification expenses.

"While a D&O policy may provide some relief in respect of the liabilities and losses flowing from a cyber security breach it may not always respond in the manner expected."

About Marsh

ABOUT MARSH

Marsh is a global leader in insurance broking and risk management. Marsh helps clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. Marsh's approximately 27,000 colleagues work together to serve clients in more than 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and people. With 57,000 colleagues worldwide and annual revenue exceeding US$13 billion, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a leader in providing risk and reinsurance intermediary services; Mercer, a leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a leader in management consulting. Follow Marsh on Twitter @MarshGlobal, or on LinkedIn, Facebook, and YouTube.

MARSH

For more information about how you can benefit from our services, please contact your Marsh adviser or call: **1800 194 888** or visit our website at **marsh.com.au**

Melita Simic | Managing Principal
Ph: +61 2 8864 7650
Email: Melita.A.Simic@marsh.com