DUAL

making relationships count

CYBER LIABILITY & PRIVACY PROTECTION UPDATE

Put simply, Cyber Liability and Privacy Protection Insurance covers a business for the cyber exposures it faces.

What does Cyber Liability and Privacy Protection Insurance cover?

Cyber Liability and Privacy Protection Insurance covers a business for the cyber exposures it faces from both **third party claims** (such as actions brought by the Privacy Commissioner, or clients suing for breach of privacy) and **first party cover** including Business Interruption and **other expenses** the Insured might incur as a result of a cyber attack. The first party expenses an Insured might incur include, but are not limited to, costs to repair or restore its systems, credit monitoring services if data has been breached, and public relations expenses.

What are the key elements of cover?

DUAL's Cyber Liability & Privacy Protection policy provides the following cover:

1. First Party Costs

The Insured's own costs to respond to the breach, including but not limited to IT Forensic Costs, Credit Monitoring Costs, Cyber Extortion Costs, Data Restoration Costs, Legal Representation Expenses, Notification Costs and Public Relations Costs.

2. Third Party Claims

The Insured's liability to third parties arising from a failure to keep data secure, including data held on behalf of the Insured by either an outsourcer, or cloud service provider for which the Insured is legally liable. Coverage is available for claims for compensation by third parties, investigations, defence costs and fines & penalties for breaching the Privacy Act.

3. Business Interruption

Reimbursement for the Insured's lost profits resulting from a Business Interruption Event. Unlike many of our competitors, coverage is not just limited to malicious attacks. Coverage is available for Business Interruption Loss arising from unauthorised access, any damage to the Insured's data (including data held on behalf of the Insured by either an outsourcer, or cloud service provider for which the Insured is legally liable) and/or programs, and any system outage, network interruption or degradation of the Insured's network.

SYDNEY | MELBOURNE | PERTH | BRISBANE
Tel: 1300 769 772 www.dualaustralia.com.au

4 reasons why SMEs are easy targets for a cyber incident

1. Lack of Resources

Our SME clients are focused on their core business offering be it as a Real Estate Agent, Mechanic, Manufacturer or whatever industry they specialise in. SMEs often lack the resources or expertise to understand their cyber exposures.

2. Less Educated on Cyber Risks

Large organisations provide training to employees on the importance of cyber security and the key risks to be aware of. Simple mistakes like lost smartphones, or accidentally sending an email to the wrong person, are the cause of 42% of cyber incidents*.

* Symantec 2015 Internet Security Threat Report, Volume 20

3. Weaker Network Security or IT Infrastructure

SMEs typically handle their own IT systems and security themselves, or outsource to someone as they lack the expertise.

4. SME's hold Valuable Data

There is a common misconception that SMEs don't think they will be a target of cyber threats as they have no data or information that is of value or worth stealing. SME data is more valuable than people think. Even if the SME isn't the direct target, the SME might be a great pivot point into the integrated supply chain of their valued partners.

SME claims examples

Claim Scenario 1

The Insureds computers were hacked via an email carrying malware, and the hacker was holding access at a ransom of $600. Both business locations could not access their networks and there was no sign of compromise of Patient or HR data. Fortunately for the Insured, during the rectification process both practices were able to function normally by using paper records. IT forensics were consulted and advised the Insured to pay the ransom as their work could possibly take longer and incur higher costs.

Total Paid: $26,820, less the Retention of $1,000.

Claim Scenario 2

The Insured Recruitment Agent had 3 separate data breaches over 3 year period. Hackers gained access to computer system and obtained 500 on-hired contractors bank account and drivers license details.

Total Paid: $75,000 of forensic and legal costs, and costs of notifying the affected individuals & credit monitoring services.

Claim Scenario 3

The Insureds computer systems were hacked twice which caused disruptions to the business and the need for IT specialists to respond in both instances and restore the systems.

Total Paid: Reimbursement of IT specialists costs of $6,000, less the Retention of $1,000.

Claim Scenario 4

The Insured noticed they were having issues with their IT systems and it was later diagnosed by the software supplier as ransomware. The Insured retained IT specialists to repair and replace hardware and software damage as a result of the attack.

Total Paid: DUAL paid the Insured $21,000 (after Retention of $1,000) for the recovery of incurred costs.

What laws & regulations govern Cyber and Privacy risks?

- Privacy Act 1988
- Other than the Privacy Act 1988, there are number of other Australian laws that relate to privacy including but not limited to:
- The Information Privacy Act 2014 (ACT)
- Telecommunications Act 1997 and the Telecommunications (Interception and Access) Act 1979
- National Health Act 1953 (NH Act)
- Data-matching Program (Assistance and Tax) Act 1990
- Crimes Act 1914 (Crimes Act)
- Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act)
- Healthcare Identifiers Act 2010 (HI Act)
- Personally Controlled Electronic Health Records Act 2012 (PCEHR Act)

Scary Statistics

The cost of cyber crime in Australia was estimated at exceeding $1bn annually in 2013.

The average cost to an Australian business that has been attacked is $2.82M, with the average cost per lost record estimated at $144.

Source: Ponemon 2015 Cost of a data breach Study Australia

Ransomware attacks grew 113% with 45 times more crypto attacks.

Source: Symantec ISTR20 2015

88% of targeted malware remains undetected by traditional anti virus.

Source: Trustwave "Inside a Hackers Playbook"

1 in 9 legitimate websites have a critical vulnerability.

Source: Symantec ISTR20 2015