McCormick Harris INSURANCE

ADVICE • SOLUTIONS • SERVICE

www.mccormickharris.com.au

BENDIGO • MELBOURNE • SYDNEY • GEELONG • BRISBANE • GOLD COAST • ORANGE

McCormick Harris Insurance

Advisory Document

Cyber Breach & Data Security

June 2020

Insuring the Risks

- **Content**

  - What has happened thus far
  - What does Cyber Liability Insurance cover
  - How do the polices differ
  - Claims Examples
  - Action required

- **Hackers hitting some big names.**
  - Stuxnet Worm 2010, Iran's Nuclear Program
  - Ashley Madison, 37 million users
  - Home Depot, over 50 million credit cards
  - eBay 2014, 145 million users breached
  - JP Morgan 2014, 7 million small businesses
  - Linkedin 2016, 164 million accounts
  - Facebook…….

- **Small businesses**
  - Systems locked and ransoms demanded
  - Watching email traffic, changing details
  - Mandatory Reporting
  - Reputational damage
  - Cleaning costs
  - Loss of production
  - Third Party claims against a business of any size

• What does Cyber Insurance Cover

- **Privacy Notification & Crisis Management Expenses**
- **Data Recovery Expenses**
- **Business Interruption Expenses**
- **Data Extortion**
- **Security and Privacy Liability**
- **Multi Media Liability**

  - **Extensions**
    - **Computer Fraud**
    - **Social Engineering Fraud**
    - **Telephone Fraud Expenses**
    - **Computer Hardware Cover**
    - **Payment Card Industry Data Security Standards (PCI DSS) Cover**

- **Comments:**
  - Policies and cover varies dramatically
    - Has the Event actually happened or just threatened?
  - Social Engineering
    - Baiting, Phishing, Spear Phishing, Pretexting, Scareware.
  - Meanings/Definitions in policies
    - This is critical to the quality of different policies
  - Attacks are global blasts and may not be targeted

- **Claim** means:

- (a) a written demand for monetary damages or non-monetary relief, a request for a standstill agreement, the service of civil proceedings, or institution of arbitration proceedings received by the **Insured** seeking monetary damages or including the threat or initiation of proceedings seeking a temporary restraining order or an interim or permanent injunction;
- (b) a formal regulatory investigation;
- (c) **First Party Costs & Expenses** and **Business Interruption Expenses;**
- (d) the incurring of **Privacy Notification & Crisis Management Expenses**;
- (e) **Cyber Extortion**;
- (f) under Extension 2.1 and 2.2, a **Direct Financial Loss;**
- (g) under Extension 2.3, **Telephone Fraud Expenses;**

- (h) under Extension 2.5, **Payment Card Loss**

Some of the key coverage highlights under our preferred Cyber wording include:

- Reasonably suspected Insuring Clause language, critical cover for the new Mandatory Notification Laws.
- A broad definition of a Cyber Event, including administrative error cover.
- Up to a six month restoration period under the Business Interruption section of the policy.
- A broad definition of a Computer System including a system operated by a Third Party Service Provider on behalf of the Insured.
- $50,000 sub limit in relation to Computer Fraud Cover extension.
- $100,000 sub limit in relation to Social Engineering Fraud extension.
- $100,000 sub limit in relation to Telephone Fraud Expenses extension.
- $25,000 sub limit in relation to Computer Hardware Cover extension as a result of malware.
- $100,000 sub limit in relation to Payment Card Industry extension (if applicable for the Insured).
- Automatic Worldwide Cover on a Territorial Basis.
- Multimedia Liability cover which extends to Multimedia Content published on social media sites.

Claims Example (Privacy Notification & Crisis Management Expenses)

Background

A small medical centre with around 1,500 Personally Identifiable Records ('PIR') suffered a breach due to a cyber attack on their outsourced managed service provider. A forensic IT investigation determined that all records held by the medical centre *may* have been compromised. These records included names and addresses, as well as medical records of patients.

Coverage

Privacy Notification & Crisis Management Expenses. The total costs of the notification to individuals and the privacy commissioner, along with additional expenses such as legal and public relations costs, was $145,000.

Claims Example (Data Recovery & Business Interruption Expenses)

Background

A recruitment agency head office employee opened an email which circumnavigated their email filters. The email contained ransomware which locked their IT system down. The agency refused to pay the ransom and began working with their IT provider to restore the corrupted data. Three days later another attack occurred on another one of their servers. At this point in time all servers were taken offline to assess and temporarily control the situation.

Coverage

Data Recovery & Business Interruption Expenses. After an external IT forensic investigation, it was confirmed no personal information held on the agency's system was compromised. However, the cost to restore the agency's system over a two week period was $75,000. A claim of $50,000 in relation to loss of business income also occurred. The total cost paid in relation to the breach was $125,000.

Claims Example (Multimedia Liability)

Background

The director of a construction firm made disparaging comments against a competing construction firm over social media. The comments were in response to the director's firm missing out on a lucrative contract that was instead awarded to the competing firm. The comments questioned the other firm's ability to deliver the contract and took personal aim at the director of the competing firm and his mental state.

Coverage

Multimedia Liability. Lawyers issued a monetary demand of $100,000 against the construction company in question, stating the comments had damaged the reputation of the firm and the individual director. A settlement was finalised for $54,000, including legal costs.

Claims Example (Privacy Notification & Crisis Management Expenses)

Background

A marketing company employee emailed a group of customers to promote a new marketing package they were releasing to their customers at the end of the financial year. Instead of attaching the promotional flyer, the employee accidentally emailed a spreadsheet with sensitive customer information, including financial information.

Coverage

Privacy Notification & Crisis Management Expenses. The total costs of the notification to individuals and the privacy commissioner, along with additional expenses such as legal and public relations costs, was $138,000.

Claims Example (Social Engineering Cover)

Background

An accounts person within a transport company received an email from what they believed to be a regular vendor requesting payment for goods supplied to the company recently. The email stated that the vendor's bank details had been changed due to an ongoing audit and that payment should be made to the new bank account provided.

Coverage

Social Engineering Cover. Payment was made, however after a detailed investigation between both parties over the coming weeks, it was concluded that the email was illegitimate and the money could not be recovered. The total loss to the transport company was $63,000, which was covered under the policy.

McCormick Harris
INSURANCE
ADVICE • SOLUTIONS • SERVICE

www.mccormickharris.com.au

BENDIGO • MELBOURNE • SYDNEY • GEELONG • BRISBANE • GOLD COAST • ORANGE

Why McCormick Harris Insurance?

- A Business established in 1996
- We now place premiums into the Australian and London markets around $30mill.
- Offices in Bendigo, Melbourne, Sydney, Orange, Brisbane, Gold Coast.
- We act for over 4,000 clients, across a range of varied occupations and professions.
- We place over 8,500 policies annually, of them over 4,000 are business related.
- We are a business ourselves and we know how to advise and insure business risks.

- **How you build your business is your business…..**
- **How you insure it is ours……..**