Network Security & Privacy Insurance

Why this is important

A network attack or data loss can have a direct negative financial impact on a company. This can be measured in reputation damage, unbudgeted costs, revenue loss and third party claims.

Business today is highly reliant on the internet however traditional insurance policies have not kept step and do not respond (adequately if at all) to technology related risks.

Firewalls aren't enough!

All companies hold sensitive information and data in many forms, including financial records, employee payroll, bank account information and intellectual property. There is a heavy reliance on security protocols to protect the data stored on networks and other electronic devices. However, the value of this data encourages criminals to create new ways to steal this information or disrupt networks for illegal purposes.

What is the cost impact on your business?

Your Own Loss

- **Breach costs**
  - Forensic specialists – investigating how and which records have been breached
  - Notification expenses – advising customers their information has been stolen
  - Call centre expenses – resource to speak to concerned customers about their rights
  - Credit monitoring services – watching to see if stolen data is being used fraudulently
  - PR consultants – managing communication to clients, general public and media
  - Lawyer's advice – legal obligations and defence of any claims
  - Regulatory costs – investigation and representation costs, fines and penalties, dealing with the Privacy Commission

- **Hacking and virus damage costs**
  - IT specialists – damage assessment, containment and restoration of data or networks

- **Loss of revenue**
  - Inaccessible network
  - Important systems, software or data unavailable
  - Inability to transact sales or fulfil orders, service or undertake important processes

Loss to Third Parties

- Financial loss from fraud, prevention costs
- `Specialist's costs including legal, forensic and monitoring
- Credit or tax issues
- Reputation damage
- Goodwill

The first 12 to 24 hours in a crisis

A pre-agreed strategy to outsource your response (forensic analysts, media consultants and others) will be the key to minimize disruption. Insurers are looking to add value to their insurance products by identifying experts who can provide the necessary team response.

What scope of insurance is available?

Policy wording responses and coverage availability vary significantly between insurers. Aon can assist you to select the policy which works best for your situation to assist you to match coverage to your particular protection needs.

In general terms coverage can be tailored around the following exposures:

- **Security and Privacy**
  - Privacy breach / security breach / breach of privacy regulations
  - Unauthorised disclosure of commercial / private information
  - Theft of data and identity theft including loss of employee data
  - Failure to prevent onwards transmission of virus

- **Data recovery**
  - Security breach
  - Virus / malicious code
  - Unauthorised use of computer network
  - Accidental damage or destruction of data due to human error
  - Electrostatic build up
  - Accidental damage to hardware
  - Malfunction / failure of computer network / programming error
  - Natural disaster causing data loss
  - Failure of backup power supply

- **Loss of business income**

- **Crisis management (including public relations)**

- **Regulatory defence and penalties**

- **Data extortion**

- **Multimedia liability**

- **Technology errors and omissions**

Loss Examples

- Legal practice – a laptop was left in a taxi and a substantial privacy loss arose; and in a separate incident a virus infected and impaired multiple computers
- Healthcare – a laptop containing 1,000 particularly sensitive medical records was stolen, requiring notification to patients with potential risk of legal action
- Retail – multiple customers' credit card details were stolen by a rogue employee, requiring notification and significant credit monitoring costs were incurred
- Hospitality – a hotel computer system was hacked, over one million customers' personal information was compromised, including credit card details, names, addresses and personal preferences
- Financial institution – a stock broker suffered a denial of service attack and extortion demands

Recommendation

Please contact your local Aon broker or one of our specialist team to discuss your network security and privacy risks or for a quotation to use insurance to transfer risk off your balance sheet.

Aon New Zealand
Aon, New Zealand's largest insurance broker operates a network made up of more than 700 staff located in 75 offices servicing over 195,000 clients. Our branches are backed up by a central support office located in Auckland.