

# Cyber & Privacy Protection

## Stories from the Coalface

---

### Scenario one:

**Profile:** Travel agency with four locations, \$10M turnover and 30 staff  
**Background:** The Insured experienced three separate data breaches over a three-year period in which hackers gained access to the Company's computer system. Over 250,000 individuals' credit card information and passport details were compromised  
**Policy Response:** Privacy Protection, Breach Costs  
**Outcome:** \$1,750,000 paid for the forensic and legal costs in defending the investigation brought by the regulator and the cost of notifying the affected individuals including providing credit monitoring services.

### Scenario two:

**Profile:** Charity with turnover of \$18M and 80 staff  
**Background:** The Insured was targeted with a denial of service attack (floods a targeted system with incoming web traffic until it is virtually crippled) in the last few days of a fundraising campaign. People were unable to make donations for a day while the website was being fixed.  
**Policy Response:** Cyber Business Interruption, Hacker Damage  
**Outcome:** \$1,500,000 paid for the lost donations and rectifying the damage to the Insured's website.

### Scenario three:

**Profile:** Online Retailer with turnover of \$5M and 15 staff  
**Background:** The Insured's website was defaced and included a link to a competing retailer's website when hackers gained access to personal information of their customers and overtook their website.  
**Policy Response:** Cyber Business Interruption, Hacker Damage, Privacy Protection, Breach Costs  
**Outcome:** \$800,000 was paid for loss of income, cost to repair the website as a result of the hack, defence costs for regulatory actions by the Privacy Commissioner, and costs of notifying the affected individuals including providing credit monitoring services.

### Scenario four:

**Profile:** Law firm with turnover of \$2M and 8 staff  
**Background:** The Insured's server and client records were locked by Ransomware software. The Insured was only able to get the files released after paying a ransom of \$50,000 to hackers.  
**Policy Response:** Cyber Business Interruption, Cyber Extortion, Hacker Damage  
**Outcome:** \$150,000 paid for the loss of income, the ransom demand including consultants costs to advise on handling and negotiation of the ransom, and costs to restore the network as the hackers refused to release the files despite ransom payment.