DUAL CLAIMS EXAMPLES - CYBER & PRIVACY PROTECTION

Profile	Background	Outcome
Eye surgery clinic, 2 locations, 15 staff and $12M turnover	An employee opened an email attachment that contained a virus. Once opened an encrypted virus was spread, causing the Insured to lose access to their network. The Russian hackers demanded ransom payment in BITCOIN of $6,000. Both practises were able to function normally (albeit slowly) in terms of accepting and treating patients by using paper records. However, the business was not able to raise invoices as this is part of a paperless system. Forensic Investigators were able to recover the vast majority of data and restore the paperless system.	$90,000 in IT expenses, First Party damage and lost man hours.
Real estate agents, 6 staff and $8M turnover	The insured had a Ransomware virus enter their computer system where the hacker demanded a payment of US$500 to be made. The insured's business was unable to function normally for 7 days.	$7,440 to cover the cost of restoring information, payment, as well as lost man hours.
Family owned beverage and snack Sales and Distribution Company, 15 staff and $2M turnover	A CrytopLocker virus infected the Insureds network forcing them to take their computers offline. It was found that the virus had also encrypted company files. A second virus was then detected, which required the server to be rebooted. This resulted in critical network outage with the sales team unable to send any orders for 2 days.	$3,470 in IT expenses and lost revenue.
Diesel service and repair agents, 15 staff and $4M turnover	An employee of the Insured opened a zip file attachment to an email which deployed a variant of ransomware malware. All the files used to open the attachment were encrypted as well as the Insured's drop box files in the Cloud which included HR files and employee personal data. Engineers were able to carry on with their operations however all administrative tasks at the Insureds ceased. DUALs breach response team conducted a standard enquiry with the Insureds IT provider into the causation and scope. An investigation was carried out into whether a data compromise occurred given the hackers were able to access files which contained HR and personal data.	$5,000 for loss of man hours and IT expenses to repair systems.

Profile	Background	Outcome
Engineer, 20 staff incl 3 admin and $18M turnover	The Insured had been hit with a Ransomware virus causing the server to become totally encrypted and inoperable. The extortion demand was in BITCOIN and equivalent to $10,000. The Insured decided to pay the ransom because it was discovered that there was no viable back-up of their data to restore. Remote logins were also not possible. Once the ransom had been paid, the Insured was provided with a decryption code which restored their system.	$18,650 for IT expenses to restore the system from scratch.
Accountant, 20 staff and $3.5M turnover	A former IT contractor allegedly logged-in remotely without authorisation and deleted files on the Insured's server. They also embedded spyware and downloaded viruses onto the server. However, when the police interviewed the individual, he advised that all of his computers were stolen before the Insured's computers were hacked.	$8,000 in costs incurred while restoring and repairing the server damage caused by this incident.
Online clothing retailer, 5 staff and $2M turnover	On two occasions, in January and March 2015, the Insured's computer system was affected by a CryptoLocker virus which prevented the Insured from being able to operate as usual.	$14,000 in IT expenses to restore the Insureds systems back to the position there were in before the virus.
Real Estate agents, 7 staff and $10M turnover	The Insureds network was hacked over a long weekend. The Insured deployed their existing IT outsource arrangements to respond to the attack and sought to recover these expenses as well as any additional man hours incurred during the aftermath, to return the business to normal operations.	$8,680 for the cost of restoring the network and $2,000 in additional staff hours.
Raw materials manufacturer, 28 staff and $7.5M turnover	The Insureds system was hacked via an email they received carrying a Ransomware virus. The virus prevented them from having any access to emails and their network. The hacker held the clients system to ransom and would only release files if the client paid $12,500. The fact that the client had numerous file shares and common storage areas made their system particularly vulnerable to attack and made it easy for the hacker to encrypt nearly every file in their system.	$12,500 in ransom plus an additional $25,000 in IT expenses related to diagnosing the problem, decommissioning the old servers and installing a new network.
Catering company, 7 staff and $1M turnover	An email was sent to the Insureds main email address (found on their website) which contained a virus. It resulted in an immediate ransom demand being received and malware virus spreading through their network. All the Insureds servers were affected and they were unable to use their payroll system for 2 weeks and had to resort to manual processes. The clients IT provider identified the issue and had to install new software. Grant Thornton was appointed to work with the Insureds IT provider in the remediation plan in response to the attack.	$15,000 in IT expenses to install new software and lost revenue.

Profile	Background	Outcome
Lumber and building materials wholesaler, 9 staff and $5M turnover	The Insureds system was hacked by a CryptoLocker virus which prevented employees from opening files and accessing the public drives. DUALs breach response team investigated the matter and installed new software to prevent another attack.	$19,000 in IT expenses and lost revenue.
Steel manufacturer, 65 staff and $15M turnover	The Insureds network was infected with a CryptoLocker virus. DUAL's breach response team instructed the clients IT provider to remove all workstations and take servers off the network to cleanse them.	$10,000 in IT related expenses.
Architect, 5 staff, $1.8M turnover	The Insureds network was infected with a virus that was received via email and allowed the hacker to gain access to the Insureds website. DUALs breach response team investigated the matter and removed the virus and reinstated their website.	$5,100 in IT expenses.
Medical Company, 6 staff and $2M turnover	An email opened by an employee caused a virus to infect the system including personal information of patients. DUALs breach response team were notified and shut down the server. Data was recovered from Backup drives and new software was installed.	$17,000 in IT expenses.
Landscaper, 3 staff and $900K turnover	Insured experienced a Malware infection on their computer which required all servers to be restored. DUALs breach response team responded to the attack and cleansed the system.	$2,000 to reimburse client for IT expenses.
Insurance Broker, 2 staff and $1M turnover	A malicious code was installed on the Insureds website which resulted in them being added to a domain blacklisting site as a company that contained malware. Client engagement was affected as emails were not being received or contained warnings about their content which caused the Insured reputational damage.	$17,000 in IT expenses and reputational damage.

Disclaimer: These claims example relate to the cover provided under DUAL's Stand Alone Cyber and Privacy Protection Product.