Made possible

QBE

# CYBER CLAIMS TESTIMONIAL

## CRYPTOLOCKER MALWARE

JULY 2016

> “We received support from ReSecure (RPC and, in this case, Storm Guidance) when we suffered a cyber security incident. A crypto locker virus was quickly and effectively dealt with but there were ‘complications’ that required a further investigation. Storm Guidance demonstrated strong expertise and, in the face of a lack of key information, continued to give very clear advice whilst expediting the investigation within our company and with our suppliers. There were careful judgements needed in relation to the timing of possible reports and the clear specialist advice we received enabled us to have peace of mind that we were meeting our obligations.
>
> Thankfully we suffered no major ill effects from this incident but having ‘looked into the abyss’ we are both glad that we had the commercial judgement and foresight to secure effective Cyber Security insurance cover and keen to take important additional steps to manage the risk to our business. The detailed report received from ReSecure was clear and helpful and their recommendations have been approved by our Board and are being implemented in full.” ”

## Claims Scenario

Employee ‘A’ of Company ‘X’ was unable to access any documents on their work computer. Having reported this to their IT supervisor and on investigation, it appeared that one of Employee ‘A’s drivers had been affected by the Cryptolocker virus. (*Cryptolocker source is a spoofing email with an attachment containing the malicious code).

Coincidentally at the same time, a customer of Company ‘X’ received 3 telephone messages from an individual claiming to be an employee of Company ‘X’.

Company ‘X’ stores their data via a third party cloud provider which includes sensitive personal identifiable information including passport details, customer & employee information, credit card details etc. On investigation of Employee ‘A’s account, it appears that access had been made to this data using Employee ‘A’s credentials.

Company ‘X’ immediately took the following steps:

- Notified the ReSecure data breach response service.
- Changed Employee ‘A’s password & suspended Employee ‘A’s account
- Restored the affected driver from the last back up (5 days prior to the incident).

**Related Sections of Cover and results of investigation.**

### Section 2 – Cyber, data security & multimedia cover

- Failure of the insured to protect against unauthorised access to, unauthorised use of, a denial of service attack against, or transmission of a computer virus to, information and communication assets.

### Section 7 – Forensic Costs

- Locate source of malware
- Analyse the exact nature of the malware and establish business impact
- Ensure containment & that no further malware in the system
- Establish if a breach had occurred and potential extent of loss.

**Quantum paid: £27,000**

**QBE European Operations** Plantation Place 30 Fenchurch Street London EC3M 3BD
tel +44 (0)20 7105 4000 QBEeurope.com