

# CYBER ATTACK RESPONSE

# DAY 1

— 08:00 *Client contacts Centor to report a potential global cyber attack.*

— 08:30 *Cyber attack looks likely. All systems are compromised. The client is unable to trade.*

— 08:40 *Centor contact the client's insurer and alerts the insurer's specific cyber response team.*

— 09:00 *Law firm Kennedys are instructed to lead the cyber breach response.*

— 09:10 *IT forensics instructed to ascertain extent of the attack.*

**09:15** *Media experts appointed to communicate to both internal/external audiences.*

**09:30** *ICO, along with their global equivalents, given notification of the situation.*



...**...DAYS 1-2**

*IT experts start to drill down on the 'how' and 'what' of the attack.*

...**...DAY 3**

*Ransom negotiators instructed - they give insights into the criminal gang and their traits.*

...**...DAYS 3-6**

*Evaluation of the extent and potential financial loss and exposure is gauged. Discussions of if, and when, the client will continue trading.*



# DAY 6...

*A complete analysis shows that the attack is severe.*

*Backup files are deemed insufficient - the business will not survive without discussions with the threat actors*

*The client's insurer agrees to pay the threat actors their ransom, after discussions by the ransom negotiators who reduce the original ransom amount. The final sum is agreed at \$500,000.*

# DAY 7...

# DAYS 7-14...

*After payment, the encryption key is sent, allowing full access to the compromised servers. Client is 'back on their feet' and trading efficiently.*



# 1 MONTH-6 MONTHS

- ✓ *Better systems and processes are in place.*
- ✓ *The regulatory review by the ICO and their global equivalents continues.*
- ✓ *The client's Business Interruption insurance included the services of an accounting firm who support the BI claim and presented their case favourably.*
- ✓ *BI insurance paid out.*
- ✓ *The Betterment clause paid out, meaning better stringent systems.*
- ✓ *The client is now fully operational.*

# POINTS TO CONSIDER

- *The client's cyber insurance meant that they had immediate access to a first-class cyber response team from a diverse group of global experts, with one point of contact.*
- *Without this seamless approach to their cyber-attack, it would have taken the client several weeks to research, and instruct, these individual experts.*
- *While they did so, their business would have failed.*

# CYBER INSURANCE ROI

- *The client paid £25,000 for their insurance policy that year.*
- *They received over £650,000 of professional support.*
- *The return on investment was 1:26. Or to put it another way, for every £1 spent, they received over £26 of professional support.*



# CLIENT TESTIMONIAL

“Our systems, our I.T. infrastructure and consequently our business was compromised by a cyber-attack last year. It meant that we were unable to trade. Prior to the cyber-attack, we took I.T. security very seriously and felt our systems were robust and secure.

I don't say this lightly, but I doubt that we would be in business today if it wasn't for the expert hand of Centor - specifically their Claims Department - who took charge from the moment we called them, co-ordinated with all relevant professionals and legal teams and kept a calm countenance when needed most.”



*If you wish to discuss your cyber insurance needs, please contact your Account Manager for more information.*

*[www.centor.co.uk/services/cyber-insurance](http://www.centor.co.uk/services/cyber-insurance)*