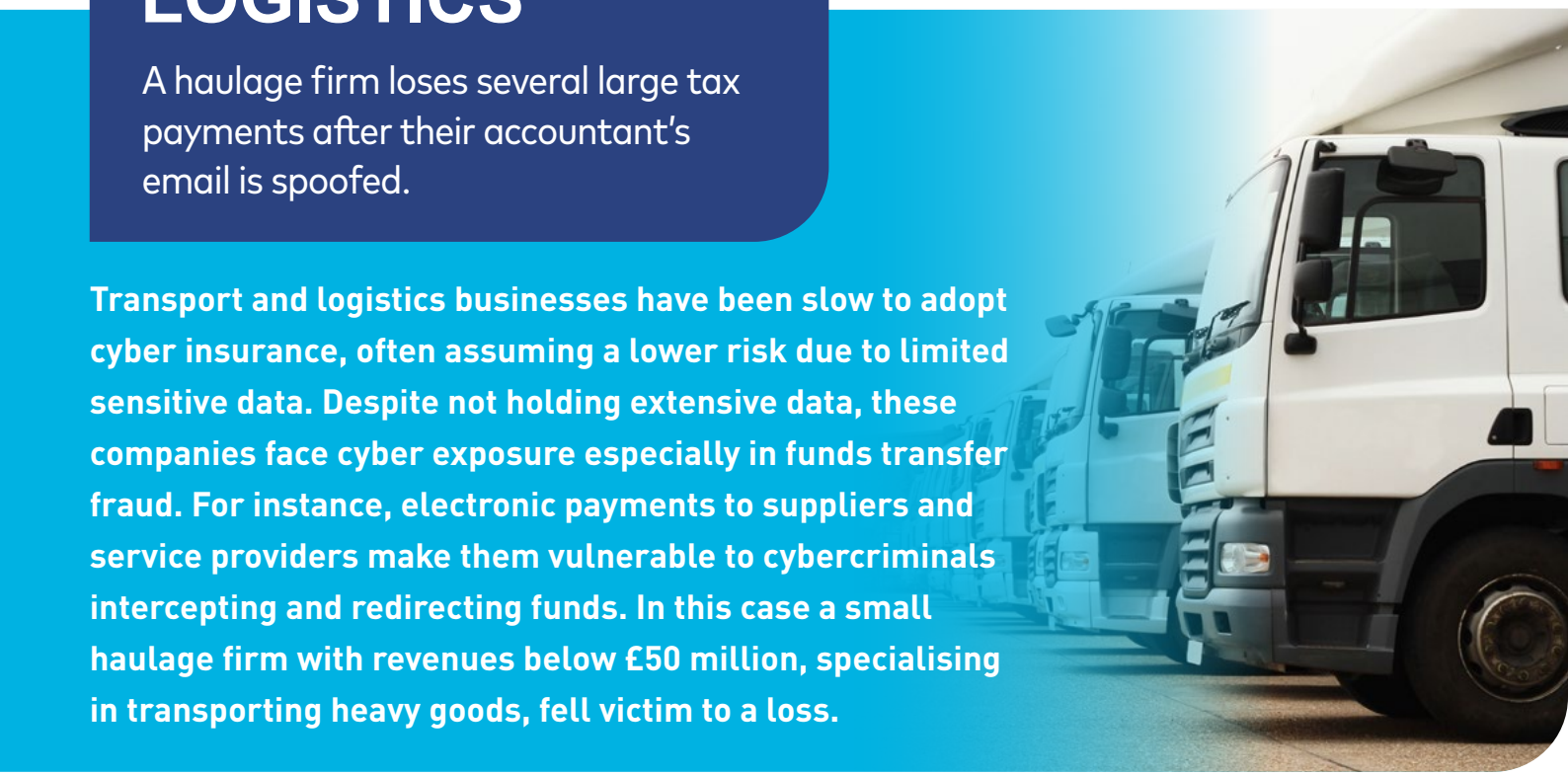
DAVID ROBERTS & PARTNERS INSURANCE BROKERS LTD

CYBER ATTACK CASE STUDY

LOGISTICS

A haulage firm loses several large tax payments after their accountant's email is spoofed.



Transport and logistics businesses have been slow to adopt cyber insurance, often assuming a lower risk due to limited sensitive data. Despite not holding extensive data, these companies face cyber exposure especially in funds transfer fraud. For instance, electronic payments to suppliers and service providers make them vulnerable to cybercriminals intercepting and redirecting funds. In this case a small haulage firm with revenues below £50 million, specialising in transporting heavy goods, fell victim to a loss.

The scam originated from email communication between the haulage firm and its accountants regarding a tax bill of £178,299. The finance director planned to pay it in four instalments due to a daily transfer cap of £50,000. After sending the first payment, the director received an email from the accountant claiming a change in bank details, leading to confusion. Despite attempting to stop the first payment, it went through. The accountant confirmed the details, and the director proceeded with the remaining three instalments to the new details, assuming the issue was resolved.

Unfortunately, a significant issue emerged. The email indicating a change in account details, sent from the accountants, was a result of email spoofing—a technique where a fraudulent sender makes an email seem like it's from a legitimate source. The fraudster mimicked the finance director's main contact at the accountancy, using a subtly altered email address for replies, preventing the accountant from detecting the scam. To enhance credibility, the fraudster replicated the accountant's genuine email signature, complete with name, job title, contact details, and an advertising banner. The finance director likely fell victim to a credential phishing scam, compromising his account security. The timing of this breach remains unclear.

Shortly after making payments, the haulage firm discovered a shortfall in taxes, prompting the finance director to contact the accountancy firm, revealing the scam. Despite immediate notification to the banks, the funds couldn't be recovered. The tax collection agency needed payment on the outstanding amount, leading the firm to pay an extra £128,299. Fortunately, the haulage firm recovered the funds through its cyber insurance policy, specifically covering social engineering losses like this.

This claim shows the increasing sophistication of cybercriminals in deceiving businesses, showcasing the challenge of discerning fraudulent activities. The fraudster utilised email spoofing, redirecting responses to a subtly different address and incorporating the accountant's genuine signature for authenticity. Such elaborate tactics make it challenging to identify scams. Additionally, the incident highlights the significant role of human error in cyber losses, emphasizing the difficulty of eliminating this risk. Despite having IT security measures, the haulage firm's finance director didn't notice the differing email address and failed to verify the account change through alternative methods. Finally, it emphasizes that virtually all modern businesses face cyber exposure, even those not solely reliant on computer systems. The haulage firm, though not primarily tech-focused, fell victim to a £128,299 fraud due to accountant impersonation. Having a cyber insurance policy allowed the company to recover the loss, emphasising the valuable protection such policies offer to any modern business.