Case study

Tax return trauma

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

Compared to many other sectors, businesses that operate in the transport and logistics industry have typically been slower to purchase cyber insurance policies. Because most transport and logistics companies don't hold large amounts of sensitive data, and because many perceive cyber insurance as primarily dealing with the cost of a data breach, many businesses working within this area don't believe themselves to be overly exposed to cyber risk.

Nevertheless, even if a business doesn't hold vast quantities of data, it still likely has some form of cyber exposure. For example, most modern businesses will use email to communicate with customers and suppliers and use bank accounts to receive and disburse funds electronically.

The transport and logistics sector is no different, and one area where they are particularly exposed is funds transfer fraud. Most transport and logistics companies will be regularly receiving and disbursing funds, not only to suppliers and subcontractors directly involved in the manufacture, sale and transportation of goods, but also to other organizations, such as accountants, lawyers and tax collection agencies. If the company makes any of these payments electronically, then they can fall prey to cybercriminals who are always looking for opportunities to intercept these funds and divert them to fraudulent accounts.

One of our policyholders affected by such a loss was a small haulage firm with revenues below $50 million. The firm specializes in the transport of heavy goods, such as cars, machinery and bulk liquids.

Tax agency changes account details

The scam stemmed from email correspondence between the haulage firm and its accountants. The haulage firm's finance director had recently been in discussion with the firm's accountants about a tax liability bill from the previous financial quarter that needed to be paid to the government agency responsible for tax collection. The amount of tax owed amounted to $178,299. Due to transfers out of the firm's corporate account being capped at $50,000 per day, **the haulage firm intended to pay this in four installments**, with three payments totalling $50,000 and one totalling $28,299.

The finance director arranged for the first installment to be transferred over to the tax collection agency. Shortly after this, however, the finance director received an email from his contact at the accountancy, stating that **he had been informed by the tax collection agency of a change of account details**. The finance director responded by email and stated that he had made arrangements for the first payment to go to the old account details and asked whether this payment would need to be stopped. The accountant responded promptly and stated that the first installment and all future installments should be paid into the new account. The finance director contacted the bank to see if they could halt the first installment.

The next day the finance director was contacted by the bank and told that it was too late to stop the first payment. The finance director emailed the accountant to let him know that the first payment had already gone through to the old account, but went on to explain that he would look to send the other payments to the new account. With the accountant confirming that this would be fine, **the finance director arranged for the next three installments to be transferred over to the new account** over the course of three days. With the payments made, the finance director assumed that the matter was settled.

Spoofed emails uncovered

Unfortunately, however, there was a serious problem. The email that had supposedly been sent from the accountants about the change of account details was actually sent by a fraudster, using a method known as email spoofing. Simply put, **email spoofing is when someone sends an email from one email address but labels it as being sent from a different address**. Fraudsters use programmes or websites which enable them to make an email look as though it has come from a legitimate email address, as well as allowing them to alter the address that the recipient responds to.

To add an air of authenticity, the fraudster included the accountant's genuine email signature with his name, job title, contact details and a banner at the bottom advertising the accountancy's services.

In this case, the fraudster sent an email that appeared to come from the genuine email address of the finance director's primary contact at the accountancy, whilst any response to these emails was sent to a very similar looking email address set up by the fraudster. So whilst the emails sent by the fraudster appeared to come from the accountant's genuine email address of joe.bloggs@xyzaccountants.com, any response to that email would automatically be sent to joe.bloggs@xyzacccountants.com, thus ensuring that the accountant wouldn't see the finance director's responses to the emails and uncover the scam. To add an air of authenticity, **the fraudster also included the accountant's genuine email signature**, which included the accountant's name, job title, contact details and a banner at the bottom advertising the accountancy's services.

Given that the fraudster knew that the haulage firm had to make a payment to the tax collection agency and that the hacker had spoofed the accountant's email address rather than sending it directly from his account and using forwarding rules to prevent the scam being detected, **it's likely that the haulage firm's finance director had had his account compromised** through some sort of credential phishing scam, although when exactly this occurred was never fully established.

$128,299

An unpaid bill is an unpaid bill

Not long after the payments had been made, the haulage firm received some correspondence from the tax collection agency, stating that although they had received a payment of $50,000, the firm still had $128,299 of tax left outstanding. **The haulage firm's finance director called up the accountancy, and it was only then that the scam was uncovered**. The banks involved in the transactions were immediately informed of the fraudulent transactions, but despite their best efforts to reverse the payments, the account had been emptied and the funds were deemed unrecoverable.

In spite of the circumstances, **the tax collection agency was not willing to compromise and still expected the amount outstanding to be paid by the haulage firm**. Not wanting to get on the wrong side of the taxman, the business paid the amount owed, but doing so left them out of pocket to the tune of $128,299. Thankfully, though, the haulage firm was able to **recoup the funds under the cyber crime section of its cyber insurance policy with CFC**, which provides cover for social engineering losses such as this.

Human error driving cyber losses and more

This claim highlights a few key points. First, **it shows just how skillful cybercriminals are becoming at parting businesses from their money** and how difficult it is for people to spot a fake. In this case, the fraudster managed to make the fraudulent emails appear as though they had come from the accountant's genuine email address using an email spoofing programme; ensured that the accountant would not be made aware of the scam by making any response to the fake emails go to a very similar but subtly different email address; and used the accountant's genuine email signature to add an air of authenticity to the scam. With fraudsters going to such lengths, it makes it increasingly difficult for individuals to spot a fake.

Secondly, it illustrates how human error plays a major role in cyber losses. Many organizations don't think they need to purchase cyber insurance because they believe they have the IT security and risk management procedures in place to prevent a cyber loss. **But as with so many cyber-related events, this loss stemmed from human error** and it's very difficult for any business to eliminate this risk entirely. In this instance, the haulage firm's finance director, perhaps understandably, failed to notice that the email address he was responding to was different from the one that it appeared to come from, and also failed to verify the account change with the accountant using a method other than email.

Finally, it highlights how almost all modern businesses have some form of cyber exposure. Even though the policyholder in this case was a haulage firm that didn't solely rely on its computer systems to carry out its business operations, **the company still used emails to communicate with other organizations and made payments electronically**. All it took was the haulage firm's accountants to be impersonated for the business to be defrauded out of $128,299. But by having a cyber insurance policy in place, the company was able to successfully recover the loss, illustrating the value that cyber insurance can bring to any modern business. ●

cfcunderwriting.com

CFC Underwriting Limited is Authorised and Regulated by the Financial Conduct Authority FRN: 312848
Registered in England and Wales RN: 3302887 Registered Office: 85 Gracechurch Street, London EC3V 0AA
VAT Number: 135541330