JESSICA PILLOW

LEARNING FROM CYBER ATTACKS

What my firm did after falling prey to the actions of a hacker – and how to avoid the same fate

I was boarding a boat from Vienna to Slovakia for a summer holiday tour of the Danube when I received the call that every accounting practice manager dreads. It was one of my team alerting me to the fact they'd discovered a cyber fraud that morning. Let me tell you a few more details, in the hope that you can ensure your practice would have sufficient controls in place not to fall victim.

My team member had been receiving emails, in the normal style, asking her to pay supplier invoices for one of our clients for whom we perform bookkeeping services. The team member paid the suppliers despite them being new and the payment amounts being over the normal prescribed maximum paymount amount, which meant it had to be split in two. She did check that she should be splitting the payment due to the payment limit, but by email, which of course went to the fraudster rather than the client.

She then entered the supplier invoices into Xero but did not allocate them to the client's specific developments in the normal way, as this was not marked on the invoice. She paid out three invoices in all, each one to a new supplier and each one over the normal maximum payment amount. It was only discovered because the client looked at Xero.

There is no doubt that although the original cause of the fraud was hacking of our client's email system, it was only successful due to weak systems at Pillow May. Our client has been extremely generous and made time to help us improve our systems. We explored exactly what went wrong and then discussed how the system could be improved. We took these actions:

1. We introduced a new engagement document, *The Scope of Bookkeeping Work*, which lists all the bookkeeping tasks that must be done for the client and notes whether the Pillow May team or a named member of the client team performs the task. This document is invaluable for appropriate delegation of tasks; it highlights any weaknesses in systems and is invaluable if anyone involved leaves!

2. We ran a bookkeeping team training session where we explored in detail what had gone wrong and discussed:

- the importance of our bookkeeping systems, such as bank reconciliations and departmental tracking, for identifying fraud as early as possible;
- the importance of understanding the nature of every transaction we process to ensure it is in line with the client's normal business dealings (this is crucial for money laundering purposes too); and
- the danger of over-reliance on email as you can never be sure who you are communicating with. Pick up the phone to ask questions!

3. We implemented dual bank authority for all bookkeeping clients, and also encouraged our clients to do the same if they handle payments internally. This is not due to a lack of trust but to stop any one person becoming liable for a fraudulent payment. With online banking apps, it is quick and easy to approve bank payments as the second signatory. If we are setting up payments for clients, we will have an additional agreement in place, which explains the invoice payment approval system and the new supplier approval process.

4. We have examined our own internal systems and introduced:

- additional security checks on our email system so it is regularly checked for automatic forwarding rules and ransomware;
- dual authentication on all our software accounts where we store client data; and
- automatic updating of all our software as soon as the latest version is released.

5. We took out cyber liability insurance which covers fraudulent payments. While we were covered in this instance under our professional indemnity insurance, if the fraudulent supplier payments had belonged to Pillow May then we would not have been covered. The insurers gave us a list of security measures to introduce into our practice, such as changing our main passwords every 90 days.

I hope that by sharing the details of our cyber attack, accountants can avoid being easy targets. Solicitors have already been targeted and have consequently tightened their payment systems. Let's make sure accountants are not the next victims. ●

Jessica Pillow, managing director, Pillow May chartered accountants