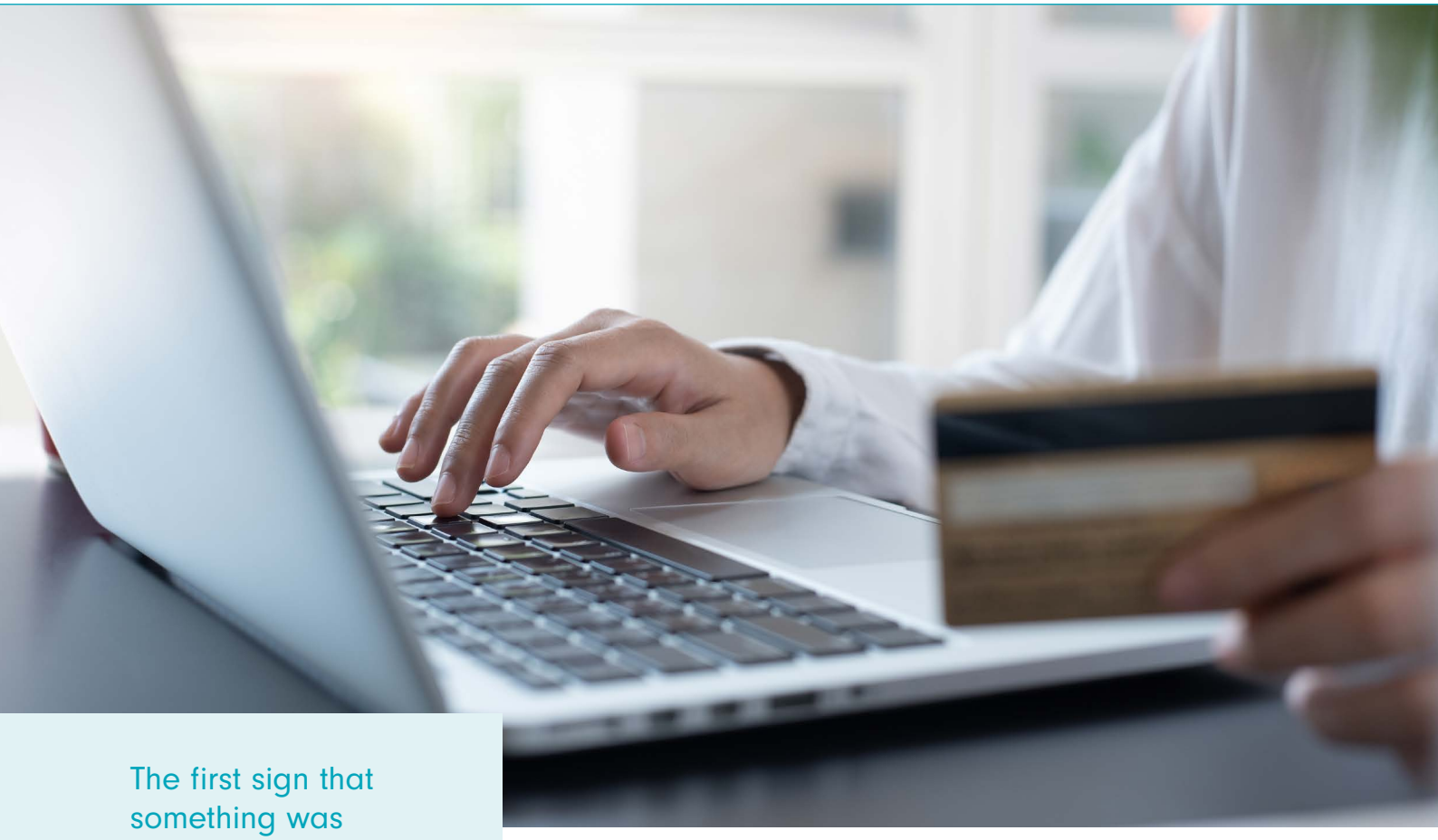
UBT TECHNOLOGY

CASE STUDY

It will never happen to you...until it does

The real story of a cyber attack on a Community business



The first sign that something was wrong came from an overdue invoice.

Not a small invoice either. The nature of Aintree Group's work in commercial and industrial design and construction means high-value contracts. In this case, $100,000.

For Phil Scarlett, a project manager at the family business in Auckland, New Zealand, it was a surprise. The customer had an excellent record of paying on time.

They received assurances that it had been paid, so they began investigating their accounts receivable.

While the investigation was ongoing, the customer paid another invoice. Money that again failed to arrive in Aintree's accounts.

With the total of missing money now reaching $200,000, the investigation became more urgent.

The customer forwarded on remittances and email communication to prove payment had been made.

It was then that Phil and Richard Scarlett, General Manager, realised something had gone terribly wrong.

Cybersecurity wasn't top of mind

"We heard others talking about cyber attacks, but we weren't close to any major breaches. We assumed our external IT provider would have everything in order," says Phil.

"Cyber attacks just weren't top of mind for our company."

Aintree aren't alone in feeling like that. Many small to medium businesses see cybersecurity as a minor issue, despite being targeted by cyber attacks at a higher rate than larger businesses.

A major reason for this higher rate is precisely because they don't have great cybersecurity systems in place.

"Many companies feel embarrassed or unsure about sharing how they also have become victims to these criminals, but here at Aintree we see it as a duty of care to fellow Community businesses to make as many as possible aware that these cyber-attacks are real," says Richard.

The attack

The email chain that shocked Richard and Phil was one advising the customer of a new bank account to pay their money into.

The email came from a legitimate Aintree address, but no staff member there had ever sent it.

That's because the attack on Aintree was both very clever and very simple.

A breach of their Microsoft 365 account (most likely via a phishing email) let the attackers into their email accounts.

They then set up what is known as Rules. Instructions for Outlook that tell it to automatically file email depending on a set of criteria.

Folders had been set up in Outlook's Deleted Items, and Rules had been put in place to automatically file any emails from the customer into those folders.

That way they could communicate with the customer from a real Aintree email, without the team ever seeing the emails.

To add credibility to the emails they created a rule to do the same for any email that came back saying it was undeliverable. Then they cc'd in Aintree management when emailing the customers, but spelt their email address with one letter wrong.

At a glance it would look like they had cc'd in management, and any undeliverable emails would bounce back into their folders in the Deleted Items.

The aftermath

"Once it was clear what happened, our attention turned to the funds we'd lost as a result. We managed to intercept 50K of the 200K that had been paid into fraudulent bank accounts, but the remaining 150K had already been transferred offshore," says Phil.

"Countless hours working with police and banks were futile in getting these funds back, and the lack of security measures at our end meant that going through an insurance provider to cover the cyber-attack wasn't an option."

As a result of this expensive lesson, they worked with UBT and enabled Multi-Factor Authentication and enhanced security on all mailboxes.

This means any sign-in on new devices or from an unrecognized IP address requires the individual to approve the sign-in from their mobile device.

By enabling this function, they immediately blocked the hackers from their compromised mailboxes, and protected them from any future breaches.

If there's one message that Aintree and the UBT Technology team can repeat, it's this.

We know cybersecurity isn't top of mind. There are a million things occupying your time, and this seems so far away.

And it is far away...right up until the point that it's not.

If you're not prepared with cybersecurity measures, you're not only vulnerable to attack, but you're not going to find any help from insurance companies.

"If you're not prepared with cybersecurity measures, you're not only vulnerable to attack, but you're not going to find any help from insurance companies."

Multi-Factor Authentication and cybersecurity awareness training for staff are two of the best ways to protect your business. UBT can help with both. Contact us today to find out more.