eftsure

Case study

Leading Food and Dairy business avoids $200k fraud

By enhancing the vendor management controls at a leading Australian food and dairy business, we ensured that our customer did not accept maliciously changed bank account details. In doing this we stopped a fraudster who, after compromising as suppliers' email, was impersonating them.

Overview

Working from Home (WFH) has transformed business operations in countless ways. However, few businesses have given much thought to the impact WFH could have on their firm's ability to prevent scams and fraud.

Luckily in June 2020, at the height of the pandemic, one leading Australian diversified food company integrated eftsure into their accounting environment. This foresight helped them avoid being defrauded to the tune of $200,000 just a few short months later.

Challenge

A routine email is all it took to potentially defraud a leading Australian diversified food company.

The food company, which regularly pays hundreds of suppliers nationwide, has a dedicated Accounts Payable (AP) team that's tasked with maintaining an accurate and up-to-date Vendor Master File.

Whilst the AP team regularly reviews supplier details, and updates them as required, they also understood that they were facing an increased risk of fraud. With fraudsters going after those organisations that regularly pay large numbers of suppliers, an organisation such as theirs was a prime target.

Furthermore, with staff working remotely due to the pandemic, the food company understood that their risk was even higher. Their staff would be using home wi-fi routers which don't have the same security capabilities as enterprise wi-fi routers, making them more prone to data breaches. Some staff may have been accessing corporate systems on personal devices, which don't have the same endpoint protections. Remote staff also tend to be more vulnerable to being deceived by email scams, as they can't easily confer with colleagues about the veracity of digital communications.

All these factors helped persuade the food company that eftsure would be a valuable addition to their AP environment.

Given the significant rise in financially-motivated fraud during the pandemic, having eftsure would allow the company to conduct independent third-party verifications of electronic funds transfer (EFT) payments in real-time before they were processed.

This would help ensure that even if a fraudster breached home wi-fi routers, personal devices or engaged in Business Email Compromise (BEC) attacks, the company could avoid losing funds to scammers.

Approach

On 13 November 2020, the food company's AP team received an email from a known contact at one of their suppliers asking to update the supplier banking details.

This known contact was a senior executive with the supplier. The AP team had been in contact with him many times in the past about various matters. The email was sent from his legitimate email address.

Nothing seemed unusual.

At this point, the food company had two methods it could use to action the change request:

a) It could use the eftsure portal to send a secure change request form to the supplier. The supplier would then need to update their banking details in the form.

b) It could update the bank details in the portal and then go through the verification process, potentially including email and call-backs, to independently verify the accuracy of the new details.

In this case, the food company opted for the latter option.

Following a period of three days, the supplier did not respond to any verification attempts, raising suspicions that something untoward was occurring. Verification attempts were complicated by the fact that all the supplier's staff were working remotely due to the pandemic. This made it challenging to contact the relevant people.

Eventually, someone purporting to be from the supplier did respond to verification attempts but was evasive and provided inconsistent details.

Finally, after repeated attempts, eftsure's team of verification experts were able to reach the original senior executive. He advised that he had not made any request to update any banking details.

This was clearly a case of attempted fraud in which the senior executive's email account had been compromised.

Result

Thanks to eftsure's tenacious and robust verification methods, it became clear that something wasn't quite right. With additional investigations, an attempted fraud was uncovered.

It is thought the scammers deliberately attempted to defraud the food company during the pandemic, knowing it would be hard for them to verify their supplier's bank details, given that all the supplier's staff were working remotely.

The food company, which had been due to pay the supplier a sum of $200,000, avoided being defrauded.

Eftsure blacklisted the scammer's bank account details, so other organisations in the eftsure system could also avoid being defrauded.