Case study

Saving a leading engineering firm over $1m

How a large construction and engineering firm used eftsure's ***Know Your Payee™*** solution to prevent a payment of over $1m to a fraudster as the consequences of a supplier's business email having been compromised by a scammer.

Overview

In the era of digital transformation our reliance on technology has become unavoidable. As with most changes, the impact is multi-faceted. Whist technology significantly increases productivity, saves time and enhances the flow of information, it can also expose businesses to new areas of vulnerability. Both newly acquired and existing data held by organisations is one such area that can becomes susceptible to attacks.

Cybercriminals know exactly how sensitive online banking data is in the 21st century. They are also persistent, resilient and patient. It's best to assume your business is constantly under a cyber-attack. Just think about all the phishing emails your spam filters caught. Eventually one will slip through the cracks. Eventually an employee will click on something they shouldn't. Or your suppliers' employee will. It only takes a single employee of any one of your suppliers to be fooled by a scammers email resulting in the supplier's email being compromised and potentially leading to your company being defrauded.

BEC scams are continuing to explode in popularity among cyber criminals, and their goal is almost always financial gain.

Challenge

One of eftsure's customers is a large engineering and construction firm that undertake large construction projects, scheduled maintenance and ongoing building service works. Their areas of expertise include project management, engineering, offsite prefabrication and integration.

Due to their diverse portfolio of services and products, the volume of invoices they pay every month is a substantial amount. As a result they recognised the risk they were exposed to and the importance of following best practice by putting in place both strong controls and eftsure's payment protection tools to help prevent fraud and error.

They signed up with eftsure in the middle of 2019 and quickly became a sophisticated user of eftsure – utilising all aspects of the solution and in particular, the supplier onboarding functionality of the eftsure portal to its utmost.

They have 19 entities set up under the one customer and their Supplier Onboarding form contains numerous pages of questions they require their suppliers to complete.

Despite the sound controls and effective payment protection software and processes they have in place, there is always a chance that their own or one of the suppliers' emails will be compromised.

The following is a recent case study of how one of their supplier's email was compromised and how using eftsure saved them from making a fraudulent payment.

Approach

At the beginning of February 2020 they had been advised of a change of account details for one of their suppliers – which is a professional company involved in providing services to the construction industry.

The requested change of banking details arrived in an email from the legitimate account of their primary contact at the supplier. It was part of a legitimate email trail the supplier and the customer had been corresponding on to discuss a particular engagement.

In keeping with the eftsure process the customer initiated a change request from the eftsure portal requesting the supplier provide their updated details via eftsure so that eftsure can independently verify them.

Since the supplier's email was under the control of the fraudster, the fraudster intercepted the email and completed the onboarding. This triggered initial internal eftsure alerts inside the verification system because the IP address of the fraudster didn't match the IP address region of the supplier and these new details differed from other banking details recently paid into for the same supplier by other customers of eftsure (A number of other internal warning flags were also triggered by the eftsure sophisticated algorithms).

Furthermore, the "supplier" had avoided use of the eftsure banklink verification process as the fraudsters knew that would immediately show the details as fraudulent.

As per eftsure's process, eftsure independently sourced the phone number of the supplier and called the supplier to verify the details. In that call eftsure were advised that the new details provided were incorrect and unknown to the supplier. eftsure immediately failed the onboarding and provided a new invitation to the supplier using a different legitimate supplier email address and advised the customer and supplier of the attempted fraud. The legitimate supplier then logged in and provided the correct details. The details were then reverified by eftsure by cross matching them to other customers paying the supplier and through another independent phone call.

After notification by eftsure, the supplier performed further investigations and found that their email account had been compromised. Fraudsters had been monitoring communication in that compromised email account and using it to attempt to defraud the supplier's customers. Once this fraud was exposed, the supplier closed the email account completely and contacted all their other customers to warn them not to accept any changed details.

The fraudulent details were added to eftsure's list of fraudulent accounts so if any other eftsure customer were to make a payment to this account, they would see a red thumb with status 'Fraudulent account'.

Results

- eftsure's Know Your Payee solution helped the customer prevent the consequences of fraud by utilising the power of community, independent verification and sophisticated fraud monitoring algorithms: Powering eftsure's verification, payment and compliance signals is our unique verified supplier database. It contains over 1.2 million verified businesses and is growing daily. It is a community of businesses protecting each other with verified vendor data.
- By verifying a change of supplier's account details with eftsure, the customer ensured payments intended for their vendor reached the actual vendor and not someone else.
- eftsure's ability to alert the customer to the fraud so quickly allowed the supplier to also notify their other customers prior to them making any payments to the fraudster Had eftsure not highlighted the fraud, the customer would almost certainly have made three payments to the fraudster as they had payments scheduled at intervals of 2 days, 7 days and 14 days from the date of the compromise. The supplier would not have queried their due payments for at least 2 weeks meaning that over $1m would have been lost to the fraudsters. This is in addition to any other payments other customers of the supplier may have made to the fraudster prior to the scam being detected.
- The comment from the customer to the supplier when asked by the supplier to supply them with the intercepted fraudulent email was : ***"Hi xxx, After searching the emails, finally I found the email telling us that you did change the banking details as per below, highlighted in yellow. Please check your email system as I think your email system has been hacked. Lucky we have eftsure to verify if this is legit. This is scary."***
- This also demonstrated to anyone that makes payments to the supplier that they are part of the community of businesses committed to solving an important issue facing all businesses in Australia.
- It was only 7 months after signing up that eftsure prevented a major loss to the customer, dramatically further proving the ROI to the customer (in addition to the productivity and workflow gains they have achieved through using eftsure).
- Real-time vendor alerts at point of payment will prevent other businesses from paying to the fraudulent account.