Sidestepping the scammers

Business e-mail compromise scams defrauded approximately USD1.3 billion from organisations and individuals in 2018 – nearly 50 percent higher than in 2017. The logistics industry is particularly exposed to scams of this nature. *Megan Ramsay* reports.

According to the annual Internet Crime Report (ICR) published by the USA's Federal Bureau of Investigation (FBI), cyber criminals defrauded some USD1.3 billion from individuals and organisation last year by means of business e-mail compromise (BEC) scams.

Fraudsters often target those who regularly transfer funds abroad and have an international network of suppliers. Logistics services providers are prime targets.

A recent warning issued by the Project Cargo Network (PCN) called on businesses to beware BEC scams, whereby criminals compromise legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorised transfers of funds, normally into a 'new' bank account.

Liability arguments

Rachel Humphrey, PCN president and ceo, said: "We understand the frustration involved if a company becomes a victim and that huge losses can be suffered, which can cause arguments regarding who is liable. Personally, I feel the banks should be taking more responsibility, or at least they should be working harder to prevent these cases.

"However, the company who fell victim should consider itself liable for the damage as it has (albeit unknowingly) transferred and authorised the payment of funds to the criminals. Therefore, the company who transferred the money is liable for the loss."

PCN pointed out that BEC is a criminal matter and any cases must be reported immediately to the police. Early discovery and reporting is crucial: cash is usually quickly drained into other accounts that are hard to trace.

We understand the frustration involved if a company becomes a victim and that huge losses can be suffered, which can cause arguments regarding who is liable.

– Rachel Humphrey, PCN

The FBI also highlighted techniques such as spear-phishing, social engineering, identity theft, e-mail spoofing, and the use of malware, all of which are part of the BEC scammers' toolkit.

Other cyber crimes to be vigilant of include cryptojacking, supply chain attacks, misconfigured cloud services and credential stuffing.

Puvaneaish Subramaniam at Malaysian freight forwarder Kagayaku Logistics outlined exactly how the company was caught out by a BEC scam.

"Our finance department received an e-mail from our Indonesian agent saying that they had changed their bank account number and to transfer to the new account. The e-mail included all the regular persons involved – but there was an extra letter in the e-mail ID that was not obvious to anyone. The dues for the month – USD4,280 – were transferred.

"We continued to receive statements from the agent to remit payment for this amount, but our finance showed proof of payment. It was confirmed that the bank account was not theirs and there had been no change of bank account. It was not

possible for us to recover the monies," Subramaniam confirmed.

The Internet Society's Online Trust Alliance (OTA) noted that although the number of breaches fell in 2018, the financial impact of cybercrime is increasing.

"While it is tempting to celebrate a decreasing number of breaches overall, the findings of our report are grim," said Jeff Wilbur, technical director of the OTA. "The financial impact of cybercrime is up significantly and cyber criminals are becoming more skilled at profiting from their attacks."

Sophisticated attack

Egypt's MGL Cargo Services is one forwarder that has suffered from this increasing level of sophistication.

Marc Gharabawi, executive director at MGL, explained: "The story started by having some troubles with the e-mail domain, receiving hundreds of spam e-mails per day. Our IT department looked for hidden viruses but found nothing abnormal. The flow of e-mails stopped and we were back to normal. This hassle took almost two days.

"Meanwhile, the hacker enjoyed browsing into our flow of e-mails, looking for money transactions. He chose a sum that was worth the headache – I think that sums less than USD50,000 were not of interest to them."

Similar to Kagayaku's experience, the scammer began by sending normal e-mails from an e-mail address that was almost identical to one belonging to an MGL agent, with just one letter altered.

"It took him at least a full week, sending normal e-mails on a daily basis, in such a way that our staff got accustomed to the new address," Gharabawi recalled.

"Then he started asking for the transfer of the money due, which is also normal. After a while, he sent us an official letter from the agent, on his letterhead paper, signed by their financial manager and even stamped, announcing the change of bank name and account.

"He kept sending e-mails three or four times a day stressing the urgency of the transfer; all the e-mails were from the financial manager of our agent. We made the transfer, according to the instructions."

Two days later Gharabawi received an anonymous phone call thanking him for the transaction. Realising something was amiss he notified the bank but, by then, it was too late and the funds had been withdrawn.

Gharabawi filed a claim with the Ministry of the Interior, which informed him that MGL's case is one of hundreds, especially among freight forwarders. The firm's case at the international court remains unresolved three years later.

Staying up to date on the latest security safeguards and best practices is crucial to preventing attacks in the future.

– Jeff Wilbur, OTA

Nevertheless, as sophisticated as the fraud is, there is an easy solution to thwart it: face-to-face or voice-to-voice communication.

As in previous years, OTA found most breaches could have been easily prevented. It calculated that in 2018, 95 percent of all breaches could have been avoided.

Wilbur observed: "Staying up to date on the latest security safeguards and best practices is crucial to preventing attacks in the future."

One example is to ensure basic online security, such as firewall and anti-virus software, is in place and current. MGL has invested in staff training to make its employees aware of the various ways in which scammers are manipulating business processes.

"Scammers exist and we have to be realistic and cope with the situation," said Gharabawi. "Importantly, we have switched all our inbound and outbound transfers to a trustable bank, where all operations are strictly revised by their HQ, and where their correspondent bank is highly ranked."

Precautions

PCN advises members to exercise caution when transferring funds and to check that notification of a change to a supplier's bank details is genuine. MGL, for instance, has told its agents that they should never accept a change of bank details unless they receive an official announcement from the managing director, followed by a phone call confirming the change.

For transfers in or out that exceed USD50,000, the accounting department calls the agent concerned over the phone to ensure that the bank details are correct.

Based on its experience, Kagayaku advises businesses to verify any new account details with the relevant party before remitting payment – and to set up several levels of internal verification and control before transacting payments.

"We have changed our standard operating procedure that any notice of change should be counter-checked by fax or by WhatsApp with the agent," added Subramaniam. Kagayaku has also moved to cloud-based data storage, with security systems in place to protect it.

In any case, PCN says payments should be monitored, and for large sums, it might be wise to pay a small portion of the total first – with the balance transferred once both parties are satisfied that it has reached the correct account.

Finally: "It is extremely important to ensure that your business insurance policy covers BEC scams, including other potential hacking and phishing scams," Humphrey stressed.