CYBER CRIME CLAIMS CASE STUDIES

Phishing scam

The financial controller of a small high street law firm received a call from someone purporting to be from the firm's bank, advising that some suspicious wire transfers had been flagged on the business account. The caller insisted that the firm may have already had funds stolen from their account and were in immediate danger of all of the remaining funds being drained unless they put a freeze on the account, for which the bank would need to be told the password and pin code.

Not wanting to be the cause of any further loss, the financial controller confirmed the pin code and password to the caller, who then confirmed that the freeze had been successfully applied and that they would be in touch again once the situation was resolved. Upon calling the bank the next day to check in, the financial controller was told that the bank had not in fact been in contact and that £89,991 had been wired to three overseas accounts in nine separate transactions. It was now too late to recall the transactions and has they had seemingly been authorised, no reimbursement was offered by the bank.

Malware theft

Hackers sent a phishing e-mail with a bogus word document attachment to a member of the accounts team within a small firm of accountants. Upon opening the attachment, a piece of key logging software was automatically installed which allowed the hackers to gather crucial access data and then log into the firm's bank portal with the credentials of one of their users.

The insured was contacted by the bank after the hackers had initiated several wire transfers and ACH batches from the insured's account to accounts located in Nigeria. After checking with the user whose credentials had been used to instruct the transactions, the firm instructed an IT forensics company to establish what had happened and to remove the malware from the system. After managing to recall some of the wire transfers, the firm were left with £164,000 lost in theft of electronic funds and costs of £15,000 for IT forensics work.

Telephone hacking

A firm of insurance brokers recently had a new VOIP (web hosted) telephone system installed in their offices to reduce call costs. Fraudsters managed to use a piece of software to crack the password to the phone network and programmed the telephone system to repeatedly make calls to a premium rate number owned by them.

One month later, the firm was contacted by their telephone network provider to confirm that they had racked up £25,000 worth of calls. Despite confirming that they had been the victims of hacking, the telephone company insisted on payment of the outstanding bill.

Ransomware

The head GP at a private doctor's surgery switched on his computer on a Monday morning to be greeted with a message stating that every single patient record on the network had been encrypted and that a sum of £30,000 was to be paid in bitcoin in exchange for the decryption key.

The insured contacted an IT forensics firm who confirmed that the level of encryption meant that it was going to be almost impossible to access the data without the encryption key and that the only other alternative was wiping the network of the ransomware which could lead to all data files being deleted. It had been a week since the last software back up, meaning critical patient data would be lost - and so the ransom was paid. Forensics were then engaged to remove any remaining malware from the network at a cost of £10,000.

CEO Fraud

A fraudulent yet almost identical looking e-mail address for the Managing Director of a medium sized building contractor was created by fraudsters who used it to instruct an individual in the accounts department to make a wire transfer payment of £50,000 to a new materials supplier. The e-mail stated that the new supplier was being used to source additional materials for a crucial job and that payment had to be made urgently to secure delivery of the goods.

The e-mail was sent whilst the MD was on holiday so that no face to face verification could be made. The account to which the funds were transferred actually belonged to the fraudsters who were able to retrieve the money before the transaction could be recalled.