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.

CLAIMS EXAMPLES

MODEL AGENCY - CRIME CLAIM

A London-based model agency with £7,500,000 in revenue suffered a major cyber crime loss after malware infected two of its computers. Masquerading as a genuine update for the company's Barclay Card reader, the malware requested that employees enter the banking pin code to enable the update to take place.

About two days after the employees entered the pin codes, it came to light that the pins had not been requested to enable an update, but to instead authorise payments to fraudsters from the business bank account. In total, £1,300,000 was withdrawn from the insured's accounts. While the bank was able to recover about £500,000 of the stolen funds, the insured was still left £815,000 out of pocket.

BRITISH RETAILER - PAYMENT CARD BREACH

A retailer suffered a payment card data breach after hackers placed malware on the payment systems at 15 of its stores, which came to light after card brands notified the company of a series of fraudelent transactions. In all, over 30,000 payment cards were compromised, which lead the retailer to incur card brand assessments totalling £345,000.

Immediately following the breach the insured carried out a PCI forensic investigation. Due to the number of retail locations affected, the cost of this reached £95,000. In addition, £31,900 in legal fees were also incurred. The total costs of the incident was £476,900.

HOTEL COMPANY – MALWARE INCIDENT

A small, independent hotel operation in the UK was the subject of a cyber attack, where they believed malware got into their own systems as a result of an employee clicking a link from an e-mail in error. Upon clicking the link, their email and accounts systems froze and they received an email message demanding the payment of a ransom fee to unfreeze their systems.

The hotel's IT company spent a couple of weeks, including weekends, to ensure the network was clear of the virus and back to normal operations. Total costs incurred to assess the damage were £15,000.

ONLINE RETAILER – SYSTEM INTERRUPTION

A retailer selling unique personalised gifts exclusively through their website and requiring the networks to be running in order to generate revenue, suffered a cyber-attack at the hands of a third party. As a result of their own data not being fully backed up as well as not having a business continuity plan that would address how to restore the website becoming operational again, they incurred total lost profit costs of £27,990 as the attack happened during their peak holiday season.

INTERIOR DESIGN FIRM – TELEPHONE HACKING

A firm of interior designers 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.

ONLINE GAMING COMPANY – BREACH OF SENSITIVE INFORMATION

An online gaming company had a DDoS attack launched against one of their websites, which repeatedly altered in real-time in order to avert the company's filters. The attack was eventually detected by a third party network team who was able to fully restore the website within a few hours, but the insured still suffered a direct financial loss as a result of the system downtime. Total lost profits during the downtime amounted to £165,000 and the company also incurred an additional $500,000 in IT costs to prevent future incidents such as this one.

INSURANCE BROKERAGE – SOCIAL ENGINEERING FRAUD

A financial controller at an insurance brokerage received an email from the managing director, who was currently out of the country on holiday. The email advised the employee that a payment of £25,119 needed to be made that day. The financial controller tried to call the MD on her mobile to check the payment details, leaving a voicemail. In the meantime, a further email was received clarifying these details.

Because the request was not uncommon and not wanting to delay things further, the employee went ahead and made the payment. Upon reviewing the request, however, he noticed that the email address didn't look quite right and that it was actually mispelled. Realising it was fraudulent, the police and bank were quickly notified, but the £25k was not able to be recovered as the money had already been withdrawn and paid into other accounts.