HISCOX

Crime insurance
Social engineering cover

Social engineering is a growing risk that many organisations are facing, as fraudsters develop increasingly sophisticated methods to defraud companies. In a typical case of social engineering, fraudsters pose as legitimate individuals, such as a company director or senior manager, a supplier, or a customer. They then leverage the social status or business relationships of the individual to gain money or information from an unwitting victim.

The frauds are often conducted via email, but can also involve written requests and phone calls and in many instances the money cannot be recovered.

Loss scenarios

Director impersonation

The head of finance at a UK marketing firm received a number of emails from his boss, a director of the firm, requesting transfer payments to be made to bank accounts listed in the emails. The company had no control procedures in place so, as the emails seemed genuine, he authorised the payments. The requests were sent over a two week period, during which time the director was on holiday.

When the director returned to the office, it was discovered that his email account had been cloned and the payment requests were fraudulent. In this instance the fraud payments totalled in excess of £100,000.

Suspect supplier

The UK finance manager of a technology company was responsible for the payments of invoices to the company's suppliers. One supplier had not been paid and so had been chasing the overdue invoice payments. Two of the emails the finance manager received from his contact at the supplier notified a change of bank details and currency for the overdue invoices. The emails included the suppliers original invoices, so he paid the overdue £35,000 in the new currency to the new bank account.

The bank then supplied a credit confirmation which showed the bank account wasn't connected to the supplier. This prompted the finance manager to review the emails and he noticed the email addresses and invoices had been slightly altered in the two emails.

How can you prevent a loss?

While no measures can eliminate the risk of suffering from this type of fraud, adopting consistent risk management controls can reduce the risk. Some robust measures to have in place, that may help (but cannot guarantee) to reduce the chance of a loss, include:

- implementation of a consistent process of dual controls for all types of payments
- authentication of invoices prior to payment, including call-back confirmations
- when any changes to employee, supplier, or customer details (such as bank accounts, correspondence or delivery addresses) are requested, ensure that a verification process is followed. This process could include call-backs to known individuals, written confirmation of the change to a pre-supplied address, or caps on first payments to new accounts
- automatic generation of exception reports showing all changes as described above, which is reviewed independently on a regular basis
- ensure processes are in place so that no one person controls payment or data change procedures from end to end
- maintain secure storage, release and/or disposal of sensitive or confidential information which could be used by fraudsters.

It is good practice to raise awareness among staff of the risk of social engineering and to educate them in the risk management measures that you have in place as the first line of defence for your business.

How can Hiscox help?

Our social engineering extension provides tailored cover to enhance our Hiscox Crime Insurance to address the specific exposures.

Cover is available with limits up to £150,000 or €150,000. **Please speak to your broker to find out more.**

HISCOX

Hiscox
22 Bishopsgate
London EC2N 4BQ
United Kingdom

T +44 (0)20 7448 6000
F +44 (0)20 7448 6900
E enquiry@hiscox.com
www.hiscoxgroup.com

16448 08/22