BRIDGE Corporate

BRIDGE
INSURANCE BROKERS LTD

Insurance innovation spanning 40 years

Crime and Fraud Insurance

The United Kingdom is seeing a huge rise in cybercrime some of which could genuinely see a company collapse. PwC recently reported that the threat of cyber offences was now a board-level issue yet it was still not being taken seriously enough by the majority of companies.

Approximately 55% of UK Firms have fallen victim to some form of economic crime in the last 2 years and cybercrime is the fastest growing area rising from 20% to nearly 50% of all economic crime in that time.

The majority of firms do not have any plans in place to fend off cybercrime which is why Bridge Insurance Brokers has negotiated access with online risk management specialist Berea to offer its clients 30 days free access to Bereas's risk management portal.

Via the risk management portal, our clients can assess their own exposure and put in place policies to reduce legal liabilities, improve security and protect their brand, whilst accessing education modules that will assist with completion of the UK Government's Cyber Essentials Scheme. Risk Management is only the beginning though and if companies have procedures in place and still suffer an economic crime loss then crime insurance is designed to pick up those losses whether perpetrated by someone on the inside or by a third party.

Whilst it can be hard to accept that your own staff might be stealing from you, unfortunately the truth is that it may be the most trusted and senior staff who have the knowledge to skirt round security and set up well concealed fraudulent systems.

Third Party fraud is also on the increase with sophisticated criminals using advanced methods of fraudulent activity to steal from your business.

AIG's Crime Solution

Standard Cover Includes:

- Employee Fraud discovered during the Policy Period
- Third Party Fraud discovered during the Policy Period
- Sub Limit for Professional Investigation Services to quantify a potential loss.
- Broad Cover for New Subsidiaries (unless US listed or US based)
- No Aggregate Limits
- No "System of Check" requirement like some other insurers. If a loss is due to an unintentional failure of a control procedure, the claim will still be paid.
- Fraud Investigation Costs

Email: enquiries@bridgeinsurance.co.uk **Website:** www.bridgeinsurance.co.uk

Fake President Fraud

Currently the most favourite fraud of the criminal fraternity affecting businesses across Europe, usually targeting finance managers, account payable clerks and other employees responsible for bank transfers. It involves impersonation of a high ranking company official, for example a Chairman or Managing Director with sufficient authority to request or approved an urgent financial transaction and persuading the employee to carry out the transfer under the pretext of an acquisition, deposits or debts.

Invoice Fraud

Another popular scam is where an email is received from what appears to be a genuine supplier informing the company of a change in bank account details and the IT systems are updated automatically, then when the genuine invoice comes in from the supplier it is paid to the criminal's bank account. Normally the fraud isn't discovered until the supplier calls to state they haven't received payment which could be 2 or 3 invoices down the line and far too late to recover anything.

Hacking

Now a traditional form of fraud whereby criminals exploit weaknesses in your IT infrastructure to access computers and ultimately software programs to transfer money from your online banking into their own accounts.

Phishing

Is an attempt by criminals to acquire sensitive information such as usernames and passwords often masquerading as a trusted entity in emails with a view to accessing bank accounts to transfer monies to their own account.

Malware

Is intrusive software normally delivered as an email attachment in the form of worms, Trojan horses, ransomware, spyware, adware and key stroke logging. It can sit on your computers without your knowledge gathering information and before you know it bank account information such as user id's, passwords and security answers are in the hands of the criminals.

Telephone Scams

Not all third party fraud is committed online however and we have seen examples whereby employees are tricked into transferring thousands of pounds in telephone scams by individuals pretending to be from the company's bank or finance providers.

Fake Delivery

We have also seen circumstances whereby third party criminals accept delivery of goods at the entrance to a company's premises then disappear without the company even knowing, until the suppliers chase payment.

Get in touch

John Batty
john.batty@bridgeinsurance.co.uk
0161 234 9357

AIG's Crime Solution

All these examples of Crime and Fraud would be covered by the AIG Crime Policy as long as Company Procedures were in place and just not followed by Individuals.