centor
INSURANCE &
RISK MANAGEMENT

Nearly 50% of all recorded crime last year was for fraud and cybercrime.

What can you do to protect your company?

It is staggering that nearly 50% of the 11.8m recorded crimes in England and Wales last year related to either fraud or cybercrime*.

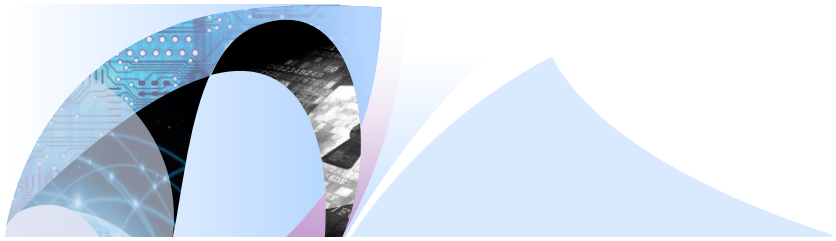
We have all come across cyber scams in our personal lives – from fake bank messages seeking your financial details, to emails apparently from reputable companies or organisations such as HMRC asking you to click a link in the email which, once clicked, allows the fraudster to place malware on your computer. This type of scam is called 'social engineering'. More often than not, the hackers have obtained personal details about you, through either social media or another online presence, and use this data to trick you into doing something of your own free will.

With company social engineering scams, the hackers are even more ingenious. An email to accounts on a Friday afternoon apparently from a senior executive about an invoice 'just received' that must be paid that afternoon. A call allegedly from the bank's technical support team asking for information to effect a software update. An email purportedly from a supplier with corrections to their bank account details.

Your company could lose thousands of pounds in just a few strokes of the keyboard. Even worse, standard insurance both general and cyber is unlikely to cover your loss, because your employees gave their consent to the transaction, albeit on a mistaken basis.

So how do you reduce the likelihood of this type of crime working, and make sure you are adequately insured for the rogue scam that does get through? Here are three key steps:

**Office for National Statistics: Crime Survey for England and Wales, 2016.*



1. Always follow best IT practice. Define and implement a thorough security policy. Adopt proper defence systems – such as spam filters, anti-virus software and a firewall – and keep these updated. Track sensitive documents.

2. Recognise that no matter how well-considered your IT security ,you are always vulnerable to the human element. So, invest in educating your employees about cyber security. Make them think before revealing information. Check 'from' addresses, beware of pop-ups and links, be extra careful of urgent financial requests. If they learn how to protect the company's confidential data, they'll be able to spot a social engineering scam. As they become more vigilant, so they become an effective security layer themselves.

3. Carry out periodic cyber security assessments. Companies evolve, grow, change — and the information flow within the organisation changes. Consequently, vulnerability testing should be carried out on a regular basis and lead to actionable recommendations to improve data security. Finally, remember the limits of standard insurance policies and consider specific cover for social engineering fraud.

Centor are specialists in this area and can guide you to the right policy for your company. Call Andrew Hogan on 0207 330 8748 or email ajh@centor.co.uk.