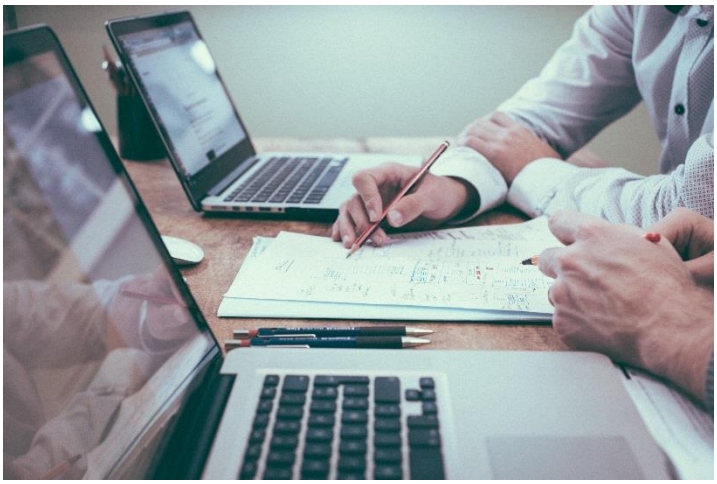
KCS Group Europe

# Hide and Seek

25th July 2017



**It has been well reported that the human factor is often the weakest link in cyber security. Even the most advanced systems are susceptible to human error. According to Kaspersky, which utilised the B2B international market research company to scrutinise 5,000 companies across the globe, the results stated that "Fifty-two percent of businesses admit that employees are their biggest weakness in IT security, with their careless actions putting business IT security strategy at risk."**

The risks posed by staff can be numerous but the most widely referenced IT risks by companies included inappropriate sharing; data on lost mobile devices; and inappropriate use of IT resources. Whilst hardly unsurprising concerns in a society where almost all businesses are online and all employees have access to smartphones, the Kaspersky report did uncover a rather more alarming fact: in the event of a cyber breach some employees would not report it, and would in some circumstances hide their mistake and leave the company to find the source of the problem. The percentage of employees attempting to hide their mistakes was higher in larger companies with staff numbers exceeding one thousand - according to the study's findings.

Kaspersky stated the reason for this appeared to be fear of a reprimand and argued for a more open and understanding environment when it comes to employees coming forth and admitting a mistake. Whilst it can be upsetting for an employee to learn that they have left their employer open to attack, ignoring the problem isn't a solution either particularly as with most problems identifying it sooner means it can be fixed before the problem escalates.

Educating the workforce to the dangers of phishing emails and social engineering is a good preventative measure for a company. The Information Systems Audit and Control Association (ISACA) stated that more than three quarters (76%) of UK office workers don't know what ransomware is and 36% can't confidently define a phishing attack. This is important as ransomware is frequently being inserted into phishing attacks. Despite the information provided by the ISACA which provides a clear deficiency in staff training however, the same survey revealed that more than half of UK office workers say that their employers have provided no cyber awareness training. This obviously has to be remedied, particularly as almost every facet of modern commerce involves some form of IT, coupled with the fact that all businesses big or small possess information that is valuable to cyber-criminals.

The other side to the same coin is fostering an understanding culture for dealing with mistakes when they are inevitably made. An educated workforce that is aware of the dangers and is unafraid to come forward when a mistake has been made will ensure that a company has a chance of eliminating a major potential weakness in a company's IT system.