Policies in action: claims examples

Social engineering

A financial controller in a law firm received a call from someone purporting to be from the firm's bank, explaining that some suspicious wire transfers had been flagged on the business account. The caller insisted that, in all likelihood, funds had been stolen and the business was in immediate danger of the remaining funds being drained unless they put a freeze on the account; a password and pin code would be required to do so.

Not wanting to cause any further loss, the financial controller confirmed the pin code and password to the caller, and the caller confirmed that the freeze had been successfully applied and that they would be in contact once the situation was resolved. Upon calling the bank the next day, however, the financial controller was told that the bank had not in fact been in contact and that $118,830 had been wired to three overseas accounts in nine separate transactions, all of which were too late to recall. Because the transactions had seemingly been authorized, no reimbursement was offered by the bank.

Fortunately, the law firm had purchased a cyber insurance policy containing cybercrime cover with social engineering and was able to recover the full amount from insurers less their policy deductible.