Cyber Crime cover from MPR Underwriting

'Cyber Crime' is generally accepted to be defined as:

- **Funds Transfer Fraud** – fraudulent instructions issued to a financial institution to pay money from an account maintained by an organisation;
- **Computer Fraud** – theft resulting from unauthorised access into a computer system;
- **Remote Access Fraud** – fraudulent use from a location, other than an organisation's own premises, of rented telephone lines; and
- **Social Engineering Fraud** – criminal taking committed by deceiving an employee into transferring, paying or delivering money; or, funds transfer fraud, or computer fraud, which involves deceiving an employee into providing security detail for operating or having access to an account held by an organisation.

However, cyber crime is still a crime and, depending on the insurer, will potentially be covered in a number of places. With MPR, this cover is exactly the same wherever it sits, which can be in one of three policies. The trigger is also the same across all policies (some cyber policies require unauthorised access or cyber event to trigger any crime cover that may be there).

The difference between the three contracts is what else is covered in addition to Cyber Crime (highlighted below).

For more information about Cyber Crime visit www.mprunderwriting.com

Cyber Crime cover from MPR Underwriting