# AGED CARE
## Planning for Cyber Risk

*Aged care organisations are an important part of the Australian economy and are growing rapidly as they rise to the challenge of an ageing population. They face significant cyber threats solely because of what they do. Cyber attacks are increasing in severity and are becoming a matter of when, not if. ATC Insurance Solutions is here to help you better understand your risk.*

## POTENTIAL EXPOSURES / RISKS

- Human Error: The vast majority of cyber events happen as a result of an employee doing something they shouldn't, either by accident or maliciously. This can be as simple as falling for a phishing campaign and unknowingly revealing passwords to a criminal, which could lead to a data breach or a ransomware attack. Another example could be not verifying payment details and therefore transferring funds to the wrong bank account, hence falling victim to Funds Transfer Fraud.
- Data Breach: Aged care organisations hold a lot of information about residents, patients and their families, which will include basic information such as names, addresses and contact details, but also health information, classified as sensitive and therefore, the consequences are greater if it is stolen. According to the Net Diligence Cyber Claims Study 2020, Healthcare organisations were the worst hit industry in terms of cyber claims, equating to 38% of all claims.
- Underinvestment: Their duty of care means that Aged Care facilities do not always have the excess funds to invest in Cyber Security - they need to spend the money elsewhere on things like medical supplies. The most probable reason for this industry to underinvest in Cyber Security, however, is lack of awareness of the cyber threats they face and the effects an event might have on their business.
- Funds Transfer Fraud: Any organisation that sends or receives money is at risk of falling victim to Funds Transfer Fraud. Cyber criminals are finding new, innovative ways of tricking people into paying fraudulent invoices or validating payment requests. Imagine paying a large invoice from a supplier, only to find out afterwards that it was in fact fraudulent and there is no way to recover the money. It can be a huge blow to any company.
- Ransomware: A ransomware or malware incident at an Aged Care facility can halt system operation, causing large Business Interruption losses, as well as incur costs for IT specialists to find, diagnose and stop the situation. A cyber policy can make all the difference when time is of the essence - the sooner specialists are appointed to help, the less damage the criminals are likely to do and the less costly the incident is likely to be.
- Reputational Damage: If an Aged Care firm has a serious cyber incident and is unable to fulfil their duties to their clients, this could affect their reputation. Public relations may be required to help mitigate the effects.

## HOW ATC CAN HELP:

- 24 Hour incident response hotline - access to cyber security experts in a time of crisis
- Claims managed in Australia by Australians
- Free commercial grade antivirus for up to 10 devices
- Operator error covered
- Funds Transfer Fraud cover available
- No excess in respect of remediation costs
- No sub-limits in standard wording
- Public Relations Costs covered
- Cyber Extortion Covered

## CONTACT:

**Lawrence Ormrod**
Senior Underwriter
E: lawrenceo@atcis.com.au
P: 02 9928 7107

**Jenny Arkell**
Senior Underwriter
E: jennya@atcis.com.au
P: 03 9258 1735

Issued by ATC Insurance Solutions Pty Ltd ("ATC") (ABN 25 121 360 978, AFS Licence No. 305802), Level 4, 451 Little Bourke Street, Melbourne VIC 3000 acting under a binder as an agent of certain underwriters at Lloyd's - EXTF120v1