RELIGIOUS ORGANISATIONS
Planning for Cyber Risk

Cyber criminals are targeting all kinds of businesses, especially Not-For Profit Organisations. They see a vulnerability in networks as an easy way to make money. Churches have their own specific exposure.

POTENTIAL EXPOSURES / RISKS

- **Funds Transfer Fraud**: Imagine making a large transfer to a partner organisation or benevolent fund, only to realise that the payment details provided were fraudulent and the money is now irretrievable. Money that should have gone to a good cause is now lining the pockets of criminals. Fake invoices are becoming increasingly more difficult to spot as cyber criminals use innovative methods to trick their suspects.
- **Digital Transformation**: Due to recent events, churches are having to find new ways of reaching their congregation, including providing virtual service and events, as well as keeping on top of their website and emails to share information. The increased reliance on networks makes protecting against a cyber event even more crucial. It also increases the risk of an event occurring.
- **Underinvestment:** A not-for-profit, lacking funds for 'luxuries', will typically under-invest in the most basic IT security, making it easier for Cyber criminals to access their systems and profiteer.
- **Human Error:** Humans make mistakes. According to a study by IBM, human error is the main cause of 95% of cyber incidents such as a ransomware attack or a fraudulent transfer. This could be as simple as clicking on a malicious link or opening a bad email attachment which could lead to a malware infection or criminals stealing data. Cyber security training is key to protect against this.
- **Ransomware**: Ransomware can bring all activities to a standstill. Criminals target small business because they are more likely to pay the ransom – they don't know what else to do. ATC provides access to a hotline giving a direct route to experts and advice for all cyber incidents.
- **Data Breach**: Data on all members of the congregation will be held, including more sensitive information about children and health information. Notification costs could build if a breach were to occur, as well as other costs associated with breach management.

Crawford® 24 Hour Incident Response Hotline – access to experts in a time of crisis

avast FREE Commercial Grade Anti- Virus with ATC's Cyber Policy

HOW ATC CAN HELP

- 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

Jenny Arkell
Senior Underwriter - Cyber
E: jennya@atcis.com.au
P: 03 9258 1777

Contact

Lawrence Ormrod
Senior Underwriter - Cyber
E: lawrenceo@atcis.com.au
P: 03 9258 1777

FOR MORE INFORMATION

ATC Insurance Solutions Pty Ltd
Level 4, 451 Little Bourke Street
Melbourne VIC 3000

Tel: 03 9258 1777
Email: cyber@atcis.com.au
Web: **www.atcis.com.au**

MELBOURNE • SYDNEY • BRISBANE

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