DENTAL PRACTICES
Planning for Cyber Risk

According to the Australian Government, Healthcare Service Providers experience more Cyber incident data breaches than any other sector in Australia. They have what criminals want - information and money. 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

- Sensitive Information: A key exposure for dentists is the amount of sensitive patient data they hold. People entrust healthcare organisations with their confidential information and expect them to keep it safe. This kind of data is very valuable for Cyber Criminals to sell on and is a reason why they specifically target the healthcare sector. It is the duty of dental practices to adhere to data protection laws set by the government; ATC's Cyber policy covers the breach of any privacy legislation.
- Funds Transfer Fraud: Any company that exchanges money is at risk of Funds Transfer Fraud, especially healthcare firms which have a large number of high value transactions occurring as part of their day to day activities. Criminals are finding new ways every day to trick you into paying fraudulent invoices or validating payment requests. According to NetDiligence, the average fraudulent wire transfer for SMEs in 2019 was $141,000. It would be harmful to any business to lose this amount of money.
- Increased Digitalisation: The increased use of technology in running a dental practice such as managing appointments online, taking payments, contacting patients and storing information all heighten the risk of a cyber attack. Using computers is a normal part of any business and we need to be prepared for the risks that this brings. The more computers are used, the more opportunity a Cyber criminal has to exploit employees or enter the system. This can lead to a data breach or a ransomware attack.
- Human Error: Most cyber breaches happen as a result of an employee doing something they shouldn't, most of the time unknowingly. Something as simple as clicking on a malicious link or entering credentials into a false site can expose your business to a ransomware attack, data breach or funds transfer fraud. Employee awareness training is key to protect against this.
- Underinvestment: Most dental practices will fall under the "Small - Medium Enterprise" category, which usually means they do not have large funds available to invest in cyber security. Even if they do, most are not aware of the risks they face until they experience a cyber-attack. For this reason, they are unlikely to be protecting themselves with some basic risk management measures that can deter Cyber criminals and eradicate the majority of cyber-attacks.
- Reputational Damage: If a dental practice has a serious cyber incident and is unable to fulfil their duties to their patients, 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
- Nil 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 - EXTF113v1