360 CYBER PROTECTION

Cover your Clients' Business Future

There is no silver bullet in protecting a business from cyber threats. Good risk management involves evaluation of exposures, management of digital assets and training, and education of staff who are accessing customer data and other parts of your system.

360 Cyber is a product that can work as part of an overall approach to protecting businesses against the financial and reputational losses caused by cyber threats.

360 Cyber provides

+ Risk management tools, including, commercial grade AV firewall and back up solution from Avast*, one of the largest security companies in the world. We help you keep your business safe from cyber attacks.
+ Market-leading end-to-end incident response. Coordinated by Clyde & Co (who have the largest, dedicated cyber team in Australia) and supported by a global network that includes forensic IT providers, forensic accountants, legal support, and public relations consultants. We help you navigate the challenge of responding to cyber criminals, managing customer data implications and maintaining your brand and reputation throughout the process.
+ Coverage that mitigates the financial impact of a cyber breach including Business Interruption Insurance. We help you manage the financial pressures of a cyber attack.
+ Legal Expenses and Liability coverage, subject to coverage terms and exclusions (such as fines), in legal action by regulators and third parties. We help to take away a significant threat to your businesses future.

Email. cyber@360uw.com.au | **Web.** 360uw.com.au/cyber

360
Cyber

Our People

JODIE PIDDINGTON
Executive Director - Cyber

Mob. +61 437 982 050
Email. jodie.piddington@360uw.com.au

Having held senior Broker relationship and underwriting roles at Allianz prior to joining 360, Jodie utilises her extensive relationship, strategic planning and risk selection skills to lead the 360 Cyber Team.

Previously Jodie was a member of the NSW NIBA Young Professionals Committee for 4 years helping to design and deliver educational events for the NSW Young Professional Insurance community. Leading 360 Cyber will allow Jodie to bring together her passion of relationships, technology and product development to successfully grow the 360 Cyber portfolio.

MARIA LAULILII
Underwriter

Tel. 02 906 1476
Email. maria.laulilii@360uw.com.au

JAMES DAO
Underwriter

Tel. 02 9056 1444
Email. james.dao@360uw.com.au

Our System

All Cyber business is transacted electronically through our 360 Compass Web Portal.

Please contact us should you wish to learn more or if you require assistance logging into the system.

Compass

Cyber Threats can impact SME's

All too often, small and medium businesses ignore the threat of cyber attacks. Whether they believe they are too small to target, they doubt that a cyber attack could do any great harm to their business, or they place too much faith in antivirus, firewall & cloud back-up protection, many SME businesses are suffering from the impact of cyber threats.

Quick facts for the 2020-21 financial year:

+ The ACSC received over 22,000 calls on the Cyber Security Hotline – an increase of over 310% from the previous financial year.
+ The ACSC issued 39 alerts and advisories to help combat urgent and critical threats, which were viewed over 7.8 million times.
+ The ACSC removed from the internet over 7,700 websites hosting cybercrime activity.
+ Business email compromise was one of the top five cybercrime categories, responsible for over 4,600 reports to ReportCyber, nearly 7 per cent of total cybercrime reports received. The average reported loss from business email compromise was around $50,600, up 54 per cent from the previous financial year.
+ Cybercrime reported through ReportCyber cost on average:
  - Small business – almost $9,000
  - Medium business – over $33,000
  - Large organisation – over $19,000
+ Commonwealth, state, territory, and local government accounted for around 35 per cent of cyber security incidents.
+ Category 4 'substantial incidents' accounted for 49% of the total number of incidents, broadly indicating that the cyber security incidents received by the ACSC increased in impact and severity from the previous financial year.

Source: https://www.minister.defence.gov.au/minister/andrew-hastie/media-releases/acsc-annual-cyber-threat-report-released

Email. cyber@360uw.com.au | **Web.** 360uw.com.au/cyber

Features & Benefits

360 Cyber Key Benefits

+ Any business interruption loss caused by a ransomware attack, a distributed denial of service attack (DDOS), operator error (accidentally deleting data), or any other virus or malware that prevents you from trading;
+ Business interruption losses and any costs to minimise a cyber extortion threat (where a third party has stolen your data or threatened a denial of service attack);
+ Any of the above that leads to your cloud or outsource provider not being able to afford you the agreed service;
+ Costs to restore your data that has been accidentally deleted, corrupted, destroyed or encrypted by a virus or ransomware;
+ Specialist I.T. Forensics to assist you in the event of a cyber loss or attack;
+ Costs incurred due to any accidental breach of copyright or defamation (libel and slander);
+ Your liability for losses caused to third parties by your transmission of any virus, malware or ransomware;
+ Your liability for the loss of any Personal Data or breach or any privacy legislation anywhere in the world.
+ In the event of a data breach we will offer IT Forensics to establish what happened, legal advice, credit monitoring (if bank or credit card details have been compromised), and Public Relations advice if required.
+ Liability for any fines and penalties imposed by any bank or the Payment Card industry following the loss of credit card data; Including all legal costs incurred protecting your against a valid claim.
+ Combined telephone hacking and bricking aggregate sub limit of AUD 50,000 sub limit at no additional premium with the excess of the standard cover applying.

Please note that the full terms and conditions of the policy wording apply, and coverage is subject to applicable limits.

Claims

What happens when I need to make a claim?

There is a 24 hour local incident response line, where you will receive advice and assistance from specialist staff within two hours of your initial call by Clyde & Co. The Incident Response

Examples of Cyber Incidents & Response

1. Stolen laptop A laptop containing lists of personal contact information is stolen.	+ IT forensics will be appointed to investigate, contain and block the insureds network from the device if possible. + Lawyers will be appointed as sensitive data could potentially be compromised and legal representation to confirm regulatory notification requirements and maintain legal privilege.
2. Extortion attempt You receive a ransomware email and it demands you pay an amount in crypto currency and if you don't pay all your data will be lost.	+ IT forensics will be appointed to investigate, contain, restore and reconfigure data if possible. + Lawyers will be appointed as sensitive data could potentially be compromised and legal representation to confirm regulatory notification requirements and maintain legal privilege.
3. Data theft An employee accesses Patient personal information and has distributed a copy of all your records to the dark web.	+ IT forensics will be appointed to investigate, contain, restore and reconfigure data if possible. + Lawyers will be appointed as sensitive data could potentially be compromised and legal representation to confirm regulatory notification requirements and maintain legal privilege. + Public Relations specialists will be engaged to provide advice, support to protect, or mitigate any damage to your reputation.
4. Upgrade error A software update was pushed to your system by a third party cloud service provider and resulted in you losing your data.	+ IT forensics will be appointed to help reconfigure any lost data from the last back up on file.
5. Deepfaking attack Criminals used artificial intelligencebased software to impersonate your executive's voice and demand a fraudulent transfer of $15,000 which was transferred to the requested bank account and then swiftly moved to an offshore account.	+ If you have taken out the optional Funds Transfer Fraud cover and receive any new, amended or differing transferring instructions from the client, (1) call the client on the telephone number held on file and (2) receive oral confirmation from the client that the transfer is valid, you will be covered for any financial loss emanating from this attack (excluding cryptocurrencies).

Email. cyber@360uw.com.au | **Web.** 360uw.com.au/cyber

360 Underwriting Solutions Pty Ltd T/as 360 Cyber **ABN** 18 120 261 270 **AFSL** 319181
Suite 3, Level 18, 201 Kent Street, Sydney NSW 2000

Email. cyber@360uw.com.au | **Tel.** 1800 411 580 | **360uw.com.au/cyber**