APPENDIX 1

What is Cyber Insurance?

Cyber insurance enables businesses to transfer the costs associated with recovery from the tangible and intangible losses related to a cyber-related security breach or similar event. Traditional insurance policies often do not cover these risks and often only accept the transference of known physical risks such as damage to equipment, stock, or locations. By bridging the gap between physical and digital risks, cyber insurance allows companies to get back online and resume normal business operations faster, minimising the cost to their recovery.

Third Party Liability Coverages

We cover the expenses to defend you and any damages resulting from your liability to a 3rd party.

THIRD PARTY SECURITY AND PRIVACY

Network and Information Security Liability	We cover the expenses to defend you and any damages resulting from your liability to a 3rd party for a security failure, data breach or privacy liability.
Regulatory Defence and Penalties	We cover the expenses to defend you and any regulatory fines or penalties from a regulatory proceeding for a security failure or data breach.
PCI Fines and Assessments	We cover the expenses to defend you and PCI fines and assessments arising from a data breach that compromises payment card data.
Funds Transfer Liability	We cover the expenses to defend you and damages arising from the distribution of fraudulent payment instructions to your vendors, business partners or clients as a result of a security failure.

WHAT IS CYBER INSURANCE?

TECHNOLOGY AND MEDIA PROFESSIONAL

Technology Errors and Omissions	We cover the expenses to defend you and damages arising from your liability to a 3rd party when the failure of your technology service or product is the cause of loss.
Multimedia Content Liability	We cover the expenses to defend you and damages arising from your liability to a 3rd party for media content related claims (such as copyright infringement, violation of privacy rights, defamation).

First Party Coverages

We cover the direct expenses and losses that your organisation incurs as a result of a cyber incident.

EVENT RESPONSE

Breach Response Services	We provide services in the first 72 hours to help you with the initial response to a cyber event including access to a 24/7 hotline, advice from legal counsel and preliminary forensic information gathering.
Breach Response Costs	We pay the costs to respond to a breach including computer forensic fees, legally required customer notification, legal expenses, credit monitoring and identity theft restoration.
Crisis Management and Public Relations	We pay the costs to mitigate other first party loss or third party liability such as public relations consultancy, media purchasing and voluntary customer notification.
Ransomware and Cyber Extortion	We cover the costs to respond to an extortion incident, including money, securities, and even virtual currencies paid.
Direct and Contingent Business Interruption, and Extra Expenses from Security Failure and Systems Failure	We cover business interruption loss including extra expenses resulting from interruption to your computer systems or to hosted computer systems, arising from a failure in security or a systems failure.
Proof of Loss Preparation Expenses	We cover the cost of a forensic accountant to help you prepare your claim for business interruption and reputational harm losses.
Digital Asset Restoration	We pay for the costs to replace, restore, or recreate your digital assets that are damaged or lost following a security failure or systems failure.
Computer Replacement and Bricking	We pay for the costs to replace or restore computer hardware or tangible equipment impacted by a loss of firmware integrity resulting from a security failure.

WHAT IS CYBER INSURANCE?

EVENT RESPONSE

Reputational Harm Loss	We cover you for your lost net profit arising from an adverse publication related to a security failure, a data breach, cyber extortion or privacy liability.
Court Attendance	We cover your reasonable expenses in attending a trial or other proceeding in the defence of a 3rd party liability claim.
Criminal Reward	We cover an amount offered by us for information that leads to the conviction of persons committing illegal acts against you that resulted in a claim under the policy.

CYBER CRIME

Funds Transfer Fraud and Social Engineering	We pay for funds transfer losses incurred as a result of the receipt of fraudulent payment instructions including through social engineering. We will also pay for loss incurred from the bank account of a senior executive if caused by a security failure at the named insured.
Service Fraud including Cryptojacking	We pay for the additional amounts you're billed by a cloud or telephony provider when you incur fraudulent charges.
Impersonation Repair Costs	We pay for the cost of removing websites, reimbursing your customers, legal and PR costs incurred as a result of fraudulent electronic communications or websites that impersonate you.
Invoice Manipulation	We cover the net costs that you are unable to collect for the provision of goods or services under a fraudulent invoice or payment instruction that has resulted from a security failure.

COVERAGES AVAILABLE BY ENDORSEMENT

Bodily Injury and Property Damage – 1st Party	We cover specified 1st party losses including business interruption loss for bodily injury or property damage arising from a security failure.
Bodily Injury and Property Damage – 3rd Party	We cover the expenses to defend you and damages arising from your liability to a 3rd party when a security failure results in physical damage or injury.
Pollution	We cover claim expenses and damages arising from pollution caused by a security failure.
Reputation Repair	We pay the Crisis Management & Public Relations costs required to mitigate harm to your reputation.

WHAT IS CYBER INSURANCE?

Coalition's Features

These are some of the tools available to help you improve your cybersecurity.

Security & Incident Response Team (SIRT)	Coalition is a cyber insurance provider with a dedicated team of cybersecurity experts available to you at all times.
Attack Surface Monitoring (ASM)	Continuous monitoring, attack surface discovery, scanning, reporting, and alerting for organisations of any size.
DDoS Prevention	Distributed denial of service (DoS) attacks attempt to make your Internet-based services inaccessible when you need them. Protect your websites and applications, and prevent disruptions from malicious traffic through our partnership with Cloudflare.
Endpoint Detection and Response (EDR)	Coalition offers a comprehensive threat detection solution, with a Coalition-negotiated discount, that includes protection from dangerous attacks such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions.

FAQs

Who is Coalition?

Coalition is the world's first Active Insurance company. The team at Coalition brings together in-depth technology, cybersecurity, and insurance expertise to help organisations assess, prevent, and respond to an emerging set of digital risks. We support brokers and policyholders before, during and after an incident occurs, taking a holistic approach to mitigating digital risk. Coalition's Active Risk Platform analyses complex sets of public data, threat intelligence, and proprietary claims information to create personalised risk assessments and threat monitoring that goes far beyond traditional insurance. Coalition now serves over 160,000 customers with Active Cyber, Active Executive Risks, and P&C policies.

How to I determine my security ranking?

Our security ranking provides a relative measure of an organisation's risk and security posture compared to other organisations we have evaluated. In order to determine the ranking of an insured, we correlate identified risk conditions with Coalition's proprietary loss and claims data. Unlike traditional security ratings, Coalition uses actual loss and claims data to identify the most significant risks that could potentially threaten that organisation. The result is not only a more accurate assessment of risk, but actionable prescriptions to help an organisation invest its resources against the most impactful remediation actions.

Where does the underlying data from Coalition's risk assessment come from?

Coalition's Active Risk Assessment and monitoring technology helps small and medium-size organisations protect themselves in a digital world. We learn from every scan, incident, and claim — building an advantage others can't match. We passively collect external data on an organisation's Internet facing IT infrastructure. We do not perform active collection of information, including penetration testing against an organisation's networks, without the explicit permission of that organisation.

What is Active Insurance?

At Coalition, we believe that all businesses should be able to embrace technology and thrive in the digital economy. That's why we've created a new way to **solve digital risk before they strike: Active Insurance**. Active Insurance combines the power of technology and insurance to provide coverage that is built for the digital economy. Active Insurance stands in stark contrast to traditional insurance, which wasn't built for the speed and amorphous nature of digital risks, leaving many organisations unprepared.

How can I learn more?

To learn more about Coalition visit coalitioninc.com, or our knowledge base at help.coalitioninc.com. As a dedicated risk management partner to our policyholders, Coalition's team of security and insurance experts are committed to helping you implement security and loss controls, all at no additional cost.

Glossary

asset	Web properties that your organisation owns, such as an IP Address, Domain, or Subdomain.
data breach	A cyber incident where your customer or employee data is accessed, and possibly exfiltrated, by a third party.
domain	Web address associated with the organisation. Example: coalitioninc.com
hosting	Some type of hosting provider or hosting technology being used in one or more of your assets.
IP address	An IP address associated with your company. Example: 1.1.1.1.
Remote Desktop Protocol (RDP)	RDP is a feature that enables employees to remotely log into their corporate computer from home. While it may be convenient for employees, RDP can also function as an open door for hackers to break into your corporate network.
Secure Sockets Layer (SSL)	SSL is a cryptographic protocol designed to provide secure communications over a computer network.
services	Technologies used to deliver services from your assets.
technologies	Technologies found being used in one or more of your assets.
torrents	Torrenting is a peer-to-peer file-sharing mechanism whereby assets that are hosted on your computers may be downloaded by other people who are outside of your organisation.