Cyber Risk Insurance Compliance Checklist

This cyber risk checklist is intended to assist businesses in identifying whether they are likely to meet the insurance requirements to qualify for minimum, intermediate and advanced levels of cyber risk insurance coverage. Full compliance may mean a greater number of insurance products are available or that insurance premiums are reduced.

Note that a comprehensive assessment conducted by a cyber risk technician is advisable should there be areas of compliance that cannot be verified or where further action is deemed necessary.

Insurance providers offering cyber risk protection products may apply additional or variable criteria when assessing whether a commercial applicant meets their requirements or needs to implement other safeguards to mitigate calculated insurance risk levels.

Identifying and Managing Cyber Risks

Business Name	
Date of Cyber Risk Assessment	
Conducted By	
Next Scheduled Review	

JERA

Cyber Risk Insurance Compliance Checklist

Minimum Cyber Risk Insurance Requirements

The below requirements are frequently applied by cyber risk insurance providers, considering whether they are able to offer a minimum or basic level of coverage. This type of insurance product may be suitable where other strategies are in place that reduce organisational risk or where the risk profile of the organisation is well-managed.

Requirement	Examples of Compliance	Verified Measures in Place	Further Action Required?
Employee emails are protected by Multifactor Authentication (MFA).	Staff must verify their identity through biometrics, keystroke dynamics or using a separately issued security code in addition to password protections.		
MFA applies to all remote access requests.	Requests for remote access to any business software, communications or networks are subject to MFA as above.		
Data is backed up off-site and, ideally, offline.	Data is backed up off-site and, ideally, offline.Data back-ups are carried out regularly, to a defined schedule, and are stored off-site and offline, ensuring data retrieval security.		
Backup should be end to end encrypted and password protected for cyber insurance.	Backups are stored with end-to-end encryption and password protection to ensure only you (and the server itself) can access the data.		
All endpoints are protected by endpoint detection and response protocols.	Tools are in place that detect suspicious endpoint activity to allow for prompt action to remove threats and minimise potential impacts.		
Software is updated on a regular basis.	All business software is updated on a defined schedule to include the latest updates, security patches and upgrades.		

Intermediate Cyber Risk Insurance Requirements

More intermediate cyber risk insurance products may command higher levels of protection to reduce the risk of a claimable loss and to defend the digital infrastructure within the business from prevalent security threats, such as phishing scams and critical data breaches.

Requirement	Examples of Compliance	Verified Measures in Place	Further Action Required?
Employees receive cybersecurity training, including simulations of phishing scenarios.	All staff receive training, either during induction and onboarding or as part of a regular training programme. Training must include phishing simulations and policies for staff to follow.		
Email filtering tools are robust.	Inbound and outbound emails to and from the organisation's server are scanned for malware, spam, viruses, suspicious links and potential imposter email addresses.		
Security measures apply to all privileged access accounts.	The business uses privileged access management security solutions that control access to restricted areas, accounts or resources.		
Business-critical and end-of-life (EOL) digital assets are segregated from the primary network, with emergency decommission plans in place.	Essential applications and those nearing an expiration date are stored separately to add an additional layer of security, with a mechanism available to decommission and shut down software in the event of a breach, malfunction or cyber-attack.		
System vulnerability scans are conducted.	Regular scans identify flaws, weaknesses and vulnerabilities within the business's software and systems to protect confidential data and prevent breaches.		
An incident response and disaster recovery plan is active.	The organisation has a published plan showing how it will retrieve critical data, restore access and recover functionality after any disaster event.		
Business computer networks are segmented.	The business uses network segmentation to provide greater control over performance, traffic and security protections.		
The business follows an information security framework.	Insurers can review the business policies, best practice standards and guidelines linked to information security risk management.		

Advanced Cyber Risk Insurance Requirements

Advanced insurance products with higher levels of coverage in terms of insured values, the scope of insurance and the areas covered by the policy will necessitate a more wide-ranging number of cyber risk prevention and management measures. Larger organisations, those with devolved working structures and with sector-specific cyber security risks, may need this type of insurance coverage.

Requirement	Examples of Compliance	Verified Measures in Place	Further Action Required?
Users should not be local admins.	Domain control and management are allocated to assigned supervisors, network management services or IT departments, removing the potential for malfunction or amendment to key security settings.		
Password management policies follow National Cyber Security Centre (NCSC) guidance.	Passwords are managed and configured according to NCSC guidelines, such as using at least two-step verification, strong and separate email passwords and combining three randomly selected words.		
Service accounts have recorded asset footprints covering domain monitoring, credentials and services.	Service accounts with non-human account access used to run automated services and processes are audited, documented and reviewed.		
The business utilises event and security information monitoring.	The company deploys security information and event management (SIEM) to detect, assess and act upon identified security threats before they occur.		
A data loss prevention tool (DLP) is in place.	Tools or systems are used that detect and prevent unsafe digital activities such as data transfer, sharing or access to sensitive data sources. Data usage is tracked, access requests are logged, and unapproved actions are blocked.		

Guide to Using the Jera Cyber Risk Insurance Compliance Checklist

- Examples of compliance are indicative – other provisions that meet the requirements of the insurance provider may be applicable. Use this column as a reference point to assess whether the protections within the business are likely to be considered compliant.

- The verified measures column allows the business to log the protections, tools, training or security used currently, ensuring insurance providers can work through a detailed log of all factors considered relevant to the requested insurance coverage.

- Further action required provides a space for the business to record any additional policies, protocols or protections necessary to qualify for the required level of coverage – where measures have been identified, these must be satisfied before an insurance process can be completed.

Full-Service Cybersecurity Protection

Data breaches, information theft and hacking are all core issues for businesses, but installing a firewall and crossing your fingers isn't a great approach.

Jera can advise on the emerging threats that are the biggest risks for your business, identify gaps in your defences, and recommend the best options to protect all devices – including BYOD and remote devices where you have a hybrid, flexible or remote team structure.

Getting ahead of your IT systems and cybersecurity before a disaster strikes is essential. Our capable technicians always aim to deliver actionable advice, unbeatable affordability and assistance to ensure you make confident, future-proof decisions about the optimal IT hardware, software, telecoms and security for your business.

For further information about cyber risk insurance, the requirements included within this checklist, or ways to improve the eligibility of your business for an advanced insurance product, please get in touch with the Jera team via www.jerait.co.uk