

CYBER RISK PROTECTION

Saving you time, money and your reputation





Consider the Digital Age

With businesses increasingly relying on technology to drive core objectives, the risk of losing money and data, or technology being denied or failing due to accidental or malicious interference has never been greater. Cyber events disrupt organisations of all sizes, across all industries, causing reputational damage, operational downtime, financial loss and legal action.





Here are five reasons why buying cyber insurance may be a smart decision for your business.

Protection from so much more than just privacy breaches

In fact, most claims in the UK are unrelated to privacy breaches. The most severe threat to a business can be falling victim to cybercrime, whereby funds are transferred fraudulently from online bank accounts, or business-critical computer systems are locked via ransomware attacks.

Protect your business from a range of exposures including:

CYBER CRIME

Cover for the electronic theft of funds, including social engineering scams where a victim is tricked into transferring funds to a criminal, and extortion.

SYSTEM DAMAGE

It's rare a breach doesn't cause some system damage. Records are compromised, data isn't saving, files are missing. Cyber insurance covers the costs you incur to determine the cause of the problem and resolve it.

FINES AND PENALTIES

Resulting from a regulatory investigation and can include Payment Card Industry (PCI) fines, penalties and assessment as a result of a payment card breach.



PRIVACY AND NETWORK LIABILITY

Defence costs and compensation you are legally liable to pay to a third party, including, for example, failure to protect data, breach of confidentiality or unintentional transmission of a virus.

BUSINESS INTERRUPTION

Cover for your loss of profit due to system outage. Cover can include your financial loss caused by reputational harm e.g. your client pulls a contract, or expected repeat business stops as a direct result of you suffering a cyber event.



It's your "emergency service" support

Your building's on fire, you call the fire brigade. Your office contents are stolen, you call the police. Who will you turn to when you suspect or suffer a breach, or your computer systems have been disabled and access to your network denied, or you've fallen victim to a social engineering scam and allowed a threat actor access to employee, third party, or commercially sensitive data?

The financial impact following an incident can be severely detrimental to businesses without the in-house resource, expertise or budget to effectively mitigate cyber risks. As part of your policy, you could receive critical pre- and post-breach risk management assistance, and instant access to:





90% of claims stem from human error

Data from the Information Commissioner's Office (ICO) shows that 90% of cyberattacks are due to human error*. Criminals frequently target the human not the technology. All it takes is for one person to accidentally click on a malicious link or fall victim to a social engineering attack, and it can easily result in your funds being transferred to a criminal, installation of ransomware, or unwittingly giving away credentials and inviting a threat actor into your system.

It could be something as simple as emailing the wrong attachment to the right person, or the right attachment to the wrong person. With the added distractions of home working, and employees under pressure to rattle through their inbox, this can make them less likely to question the legitimacy of the content. It presents threat actors with the perfect environment to attack.

No matter how robust your IT security protocols are, this will not stop humans making mistakes. You can only take measures to reduce the risk of it happening and minimise the impact to your business from losses occurring from it.

Can you afford not to?

Ultimately, in this, the digital age, business-owners must be able to demonstrate cyber risk has been addressed. Transferring the risk with insurance protection will help keep your business running, secure brand reputation and ensure you have the all-important incident response support for when the worst happens.

DON'T WAIT UNTIL YOU'RE A VICTIM!

Contact Catherine Aleppo, Head of Cyber
0208 557 2343 | catherine.aleppo@astonlark.com
www.astonlark.com/cyber

* Source: <https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/>



Performance is a trading name of Aston Lark Limited. Aston Lark Limited is registered in England and Wales, No. 02831010.
Registered office: One Creechurch Place, London, United Kingdom, EC3A 5AF.
Aston Lark Limited is authorised and regulated by the Financial Conduct Authority, No. 307663.

www.performance-insurance.com

AL-CS-PFM-025-0922