ADVANCED CYBER DEFENCE SYSTEMS

ESSENTIAL GUIDES **NO.1**

An introduction to: CYBER SECURITY INSURANCE

Cyber security insurance is a necessity for every business. Our essential guide covers everything you need to know, including why you might be denied coverage & what to do about it if you are.

Authors: Elliott Wilkes & Chris Culligan

In association with

gaws OF LONDON

Broker at LLOYD'S

Table of Contents

Cyber Security Insurance: Five Reasons You'll Get Denied Cyber Insurance

Cyber insurance is paramount when it comes to protecting your business from malicious online threats. Unfortunately, it's all too common for companies not to purchase cyber insurance cover, or to get denied when they make an application, leaving them wide open to data breaches.

In fact, the Department for Science, Innovation & Technology reported in April 2023 that 59% of medium-sized businesses and 69% of large businesses recalled some sort of cyber breach or attack within the last 12 months, costing £4,960 on average. There are a variety of reasons that companies are denied cyber insurance. Industry classes that have experienced a high loss ratio, such as Airlines, Education and Public Sector organisations, have found it difficult to find cyber cover.

It is also highly dependent on the maturity of their cyber security programme. There are some key security requirements that insurers will insist on a company implementing before considering providing insurance. The key areas that insurers are looking for are Multi-Factor Authentication (MFA), Endpoint Detection and Response, a comprehensive backup strategy, and staff training and awareness.

In summary, the five key reasons a business may be denied cyber insurance are as follows:

- Industry sector is automatically excluded (usually due to reinsurance restrictions on insurance carriers).
- Lack of training and awareness demonstrated by the proposed insured.
- Failure to adhere to insurer minimum security requirements: e.g. MFA, encryption of data, Privileged Access Management (PAM) tool etc.
- Previous claims history, particularly if a business has failed to demonstrate its willingness to improve cyber risk management procedures following an incident.
- Business operations located in a territory deemed high risk from either a cyber security or regulatory perspective.

What is Cyber Cover Insurance?

Cyber insurance - also known as cyber security, cyber attack or data breach insurance - covers your business for any legal, financial or reputational damage caused by security breaches of confidential data and cyber-attacks.

A holistic cyber insurance policy will mitigate against the inherent risks presented by cyber attacks. A good policy will provide the broadest coverage for both first and third-party losses to your company, arising from a cyber event.

Typical first-party cyber insurance coverages would include:

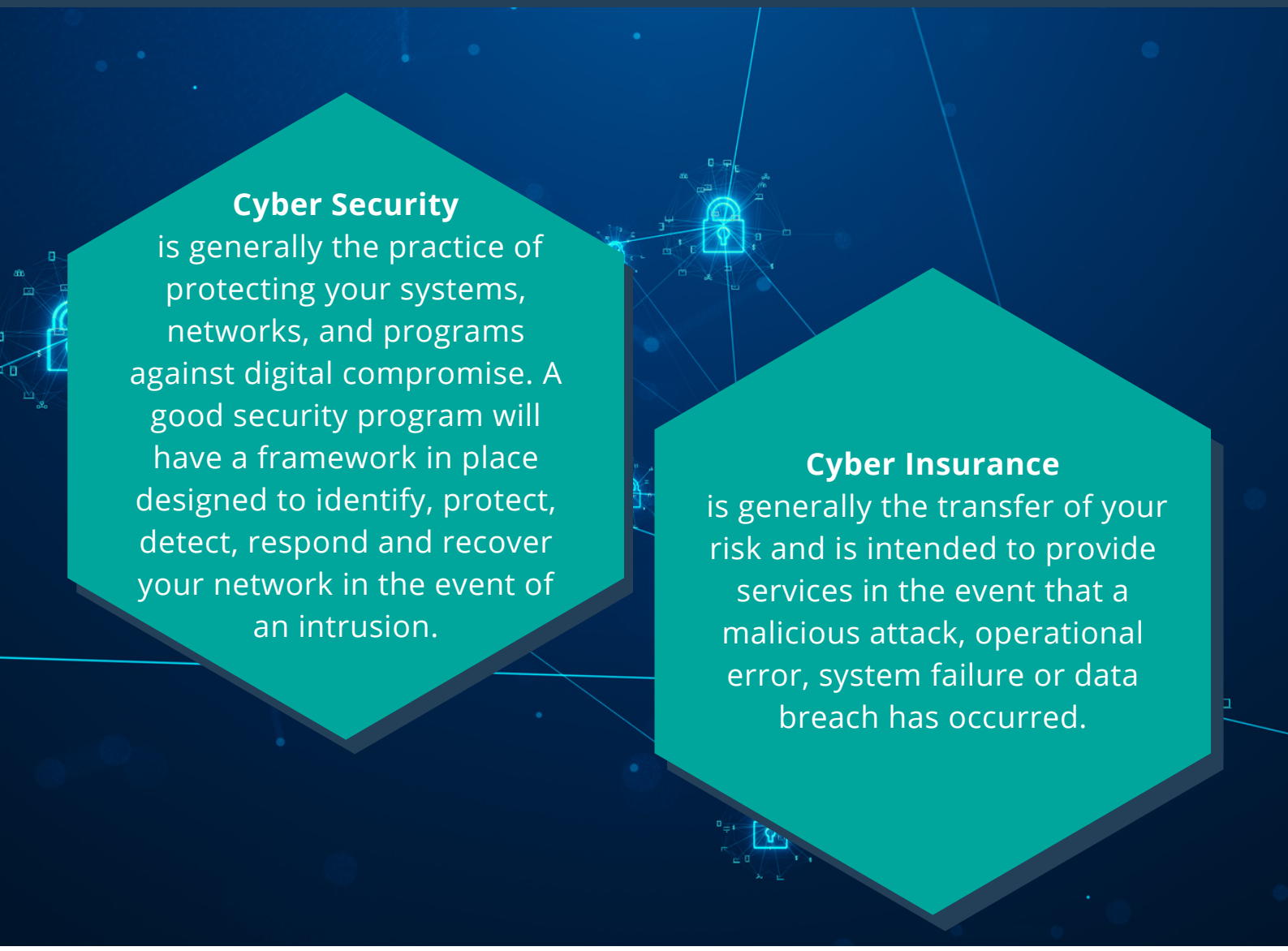
- Digital Asset Restoration Costs
- Incident Response Costs
- Business Interruption (including operational error and system failure)
- Cyber Extortion and Ransomware Costs
- Cyber Crime (including social engineering and fund transfer fraud)

Typical 3rd Party Liability costs would include:

- Data and Privacy Liability
- Customer Notification costs
- PCI DSS (Payment Card Industry Data Security Standard)
- Legal Services
- Multimedia Liability

Cyber Insurance vs. Cyber Security

Many businesses or business representatives ask the question: Why do I need cyber insurance cover if I have cyber security in place? There's a stark difference between cyber insurance and cyber security that shouldn't be overlooked.



Cyber Security
is generally the practice of protecting your systems, networks, and programs against digital compromise. A good security program will have a framework in place designed to identify, protect, detect, respond and recover your network in the event of an intrusion.

Cyber Insurance
is generally the transfer of your risk and is intended to provide services in the event that a malicious attack, operational error, system failure or data breach has occurred.

It is worth noting that a number of insurance carriers who provide cyber cover are now looking to continuously underwrite the risk to your network - known as 'active insurance'. Due to the adversarial nature of cyber, with malicious actors constantly looking for gaps in the system, they work closely with cyber security companies to provide a more rounded service.

What are the Types of Cyber Insurance?

Several types of cyber insurance policies are available, each designed to address different aspects of cyber risks and cover different exposures.

First-Party Cyber Insurance

This will cover the insured's own financial loss arising from a cyber event. A cyber event is commonly defined as any suspected or actual unauthorised access to your system, electronic attack or privacy breach.

Typical first-party cyber insurance covers the following:

1. Incident Response
2. Cyber Extortion
3. System Damage and Data Restoration
4. Business Interruption

Liability Coverage Cyber Insurance

Cyber Liability coverage, often also referred to as Third-Party cover, will indemnify companies for damages and settlements made against you, as well as covering the cost of legally defending yourself against claims of a data breach. Examples of liability coverage insurance covers the following:

1. Network Security and Privacy Liability
2. Regulatory Fines
3. Media Liability
4. PCI Liability

Recent figures have shown that the majority of costs are incurred by the insured themselves, as opposed to third parties.

Cyber Insurance policies are often modular in design, and therefore, it is important that you have the correct cover in place to address your most inherent risk.

Who Needs Cyber Insurance?

Businesses of all natures can find value in purchasing Cyber Insurance. It can protect against unforeseen risks and provide you with financial support should the worst happen.

Companies that will particularly benefit from purchasing a policy are those that operate in finance, manufacturing, and healthcare, as well as the service industry. Predominantly because these types of companies will hold sensitive customer data which, if they were to fall into the wrong hands, the company would be held responsible and potentially receive a significant fine.

Companies that operate predominantly in the online space and whose operations would be significantly impacted should their IT systems go down for any length of time should also strongly consider purchasing cyber insurance.

How Much Does Cyber Insurance Cost?

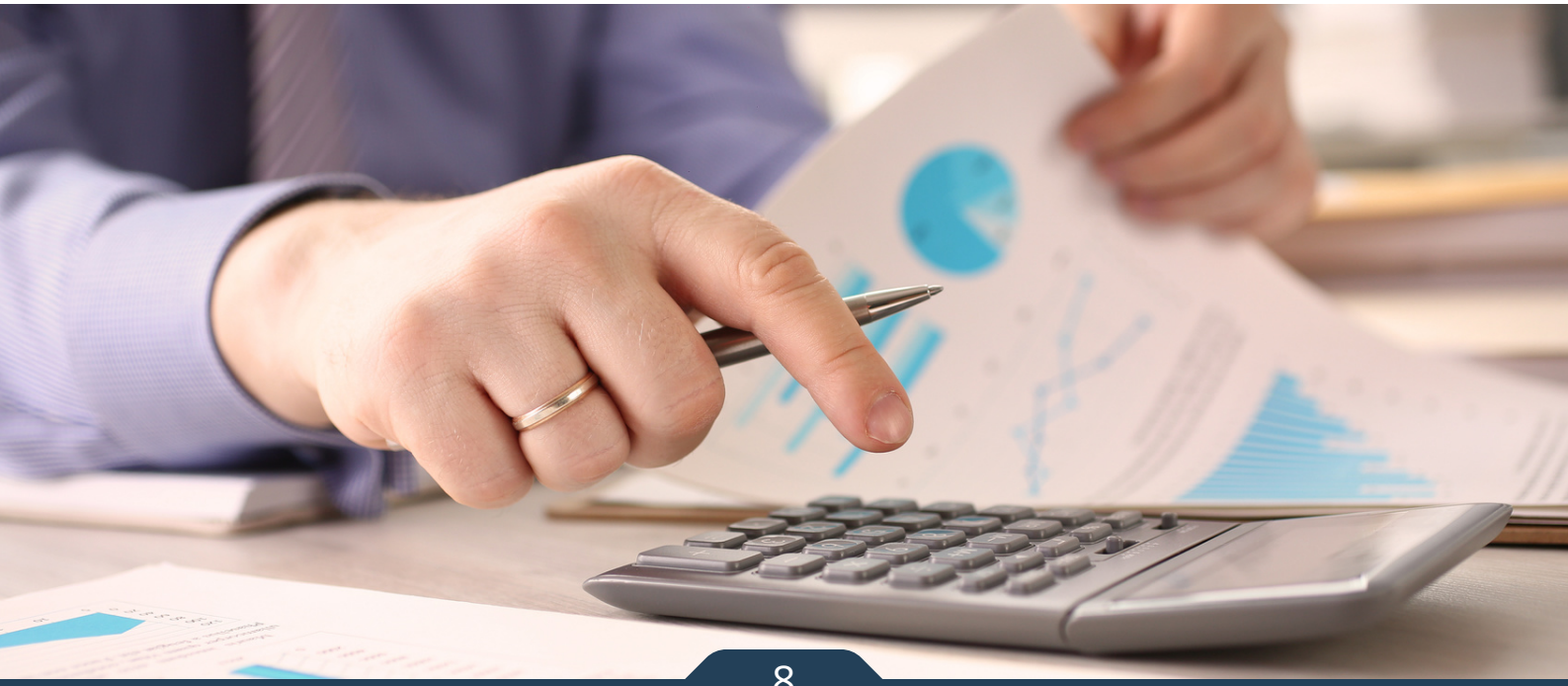
There are a number of different variables that insurers will take into account when pricing your cyber insurance policy. Some of those factors include:

1. Annual revenue and geographical split
2. Type of industry
3. Level of cyber and network security
4. Amount of sensitive customer information - 'estimated Personal Identifiable Information (PII) count'

Within Lloyd's of London, the typical minimum premiums start from approximately $15,000 per $1 million limit of indemnity purchased.

However, within the company insurer and MGA market, this can reach as low as $1,000 per million.

If you are looking to get a clearer understanding of how much a policy might cost you, then there are a number of online portals where you can run a quote against your company. For a more comprehensive view of the cyber insurance market, speak to a cyber insurance broker.



What are the Benefits of Cyber Insurance?

As previously alluded to, a comprehensive cyber insurance policy can go a long way to transferring the risk that your business holds when it comes to cyber, providing peace of mind and the ability to forecast business performance more accurately, even if a cyber event were to occur.

Financial Protection

A data breach or significant disruption in your company's business activities can have a major financial impact on your company. If this is caused by a cyber event and you have a policy in place then you can be confident that your insurer will provide both advice and financial protection to you.

In 2022, the average cost of a data breach stood at $4.35 million, whilst in the UK, it is estimated that 60% of SMEs declare bankruptcy within 6 months of a cyber attack.

Business Continuity

If you are unfortunate enough to be impacted by a cyber event, you will want to get your systems back up and running as soon as possible. A good cyber policy will be able to help you get back on your feet by covering data restoration and hardware replacement costs.

In addition to the financial protection provided within a cyber policy, insurers provide access to a vendor panel of experts on hand 24/7, 365 days a year, including IT forensic specialists, legal expertise, forensic accounting, PR and crisis communication experts and credit monitoring services.

Risk Management Support

Most insurers have either aligned with cyber security companies or have created their own in-house cyber specialists. They can offer a wide range of risk management support, including threat intelligence, network monitoring, and alerts on vulnerabilities that might impact your network.

In addition, they will have a number of pre-agreed third-party vendors who will be called upon in the event of a suspected breach. This will include legal advice, reputation management, and account forensics.

How Do You Get Cyber Cover Insurance & What's Included?

Depending on the size of your business, there are a number of ways to obtain cyber insurance.

If you are a small or medium-sized business, then you can quickly obtain a quote using a number of online portals that will provide relatively standard cover. Pricing will usually be dependent on a combination of revenue and declared risk management practices, with many insurers now also conducting an exterior scan of your network to identify any known vulnerabilities.

If you have a complex network or significant annual turnover, then you would be best served by using a broker to approach the market for you and obtain a number of quotes.

They can also provide you with benchmarking against your peers to ensure you have adequate cover in place.

A broker will also be able to talk through the coverage in more detail and assist with an onboarding call between you, your insurer, and those third-party vendors that will assist you, in the event of an incident.

Why Have I Been Denied Cyber Business Insurance?

Due to the rise in incidents of ransomware and large data breaches resulting in significant fines, obtaining cyber insurance has become a more protracted process over the last 24 months.

Average insurer loss ratios in 2019 stood around 35%, however, these spiked to approximately 130% in 2021-22, seeing a significant increase in the availability of capacity and price thereof.

While specific reasons for denial can vary depending on the insurer and individual circumstances, here are five common reasons why businesses may be denied cyber insurance coverage:

1 Poor Cyber Security Measures in Place

Probably the most common reason for not being able to obtain any cover is due to your company having a poor level of cyber security.
Most insurers will look for a minimum standard of cyber security in order to consider providing cover. These include:

- Regular training for staff on cyber security - with a focus on preventing phishing scams
- MFA across the network
- Back-ups being regularly maintained and separate from the network
- E-mail security
- Regular patching across the network

These are just a few areas that insurers will be looking for. Naturally, the larger and more complex your network, the more questions will be asked.

How to rectify poor data security measures: Contact us at ACDS today for guidance on how to introduce cyber security measures to strengthen your defences.

2 Incomplete or Inaccurate Application

Insurers will be looking for as much detail as possible when you complete your application for insurance. Any gaps in the information provided will only result in more questions being asked, resulting in considerable back and forth between you and the insurer.

Recently, there have been significant precedents set in the courts whereby insurers have refused to pay cyber claims due to an insured providing misleading information regarding their cyber security practices, most commonly in regards to the breadth of their MFA protocols and procedures, regarding the encryption of data.

3 Industry-Specific High-Risk of Cyber Crime

Whilst every business faces its own unique set of cyber exposures, hence the importance of tailoring cyber insurance policies accordingly, insurers generally view the following industries as being most exposed to certain forms of cyber risk:

1. Manufacturing/Energy/Marine: First-party cyber exposures focused on business interruption, digital asset restoration and the potential for physical damage.

2. Retail: Third-party liability exposures around customer notification costs, reputational damage, regulatory fines and penalties, and legal expenses.

3. Financial Institutions: A combination of 1st and 3rd party cyber insurance exposures encompassing both business interruption and data breaches.

4 Prior Cyber Security Incidents

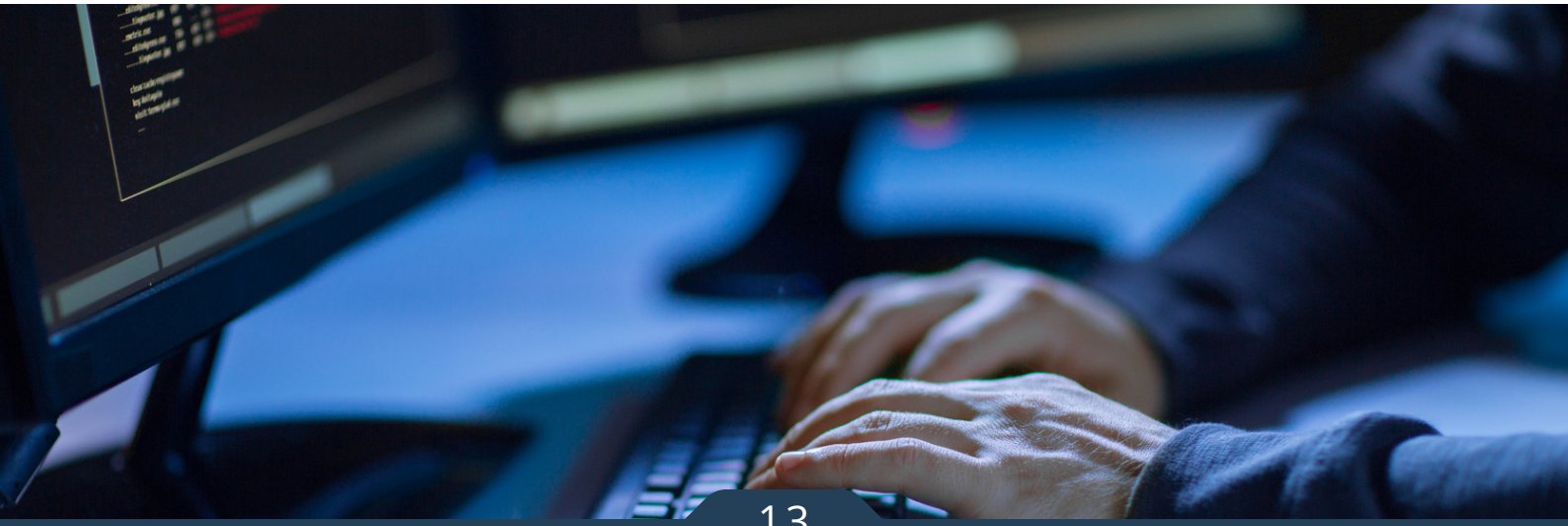
If you have previously been a victim of a cyber incident, then the insurer will likely place more scrutiny on your systems. They will expect to see a number of improvements in your processes and procedures and will want to be assured that lessons have been learned and mitigation put in place. Insurers typically request confirmation that no incidents have occurred in the past 3 or 5 years.

A previous incident is by no means a guarantee that a business will not be able to obtain cyber insurance. On the contrary, if an insured is able to clearly demonstrate risk improvements and lessons learnt from a cyber event, then this can actually improve the perspective of the risk in the eyes of cyber underwriters.

5 Poor Data Management Practices

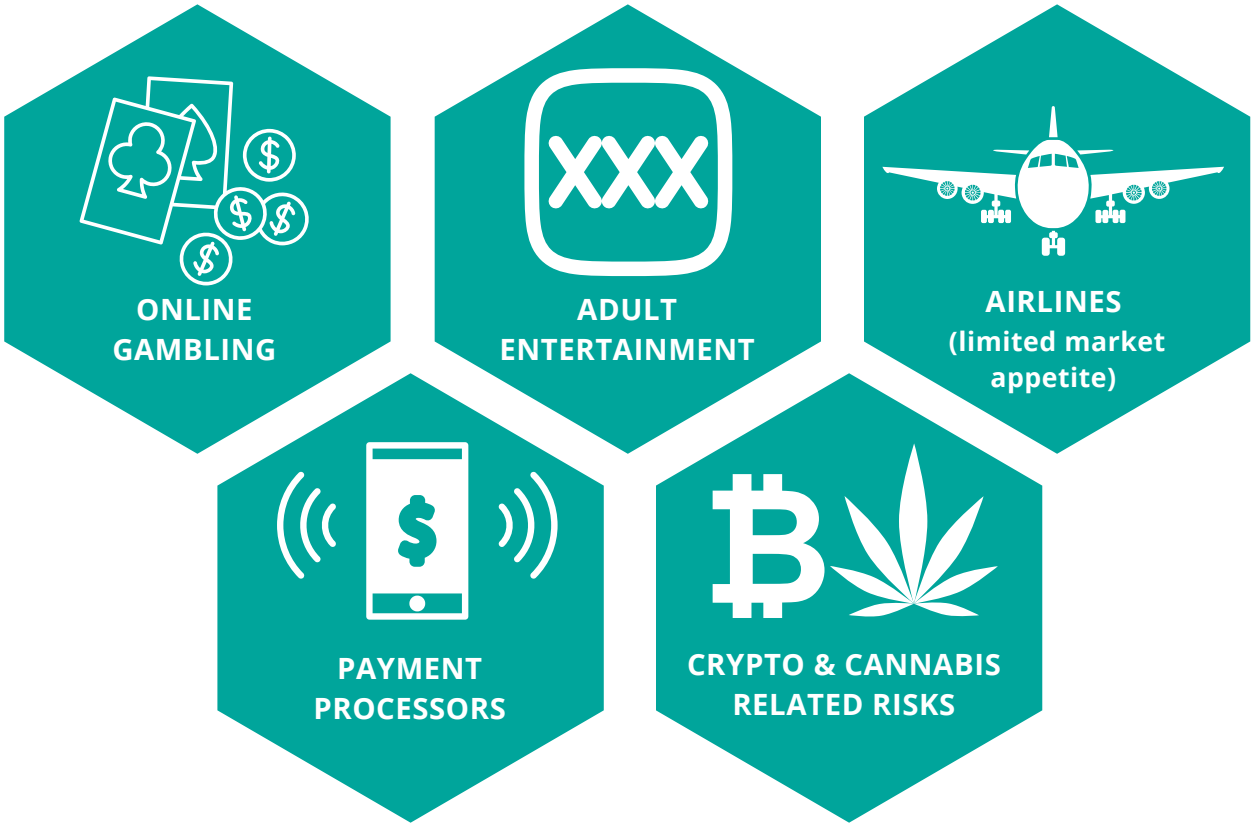
It is really all about the data, and how you manage it is vital to securing cyber cover. Insurers will want to see that your data is well managed. This usually means that it is encrypted, at rest, and in transit; any sensitive data is siloed so that there is no one data store for all data types, and access to data lakes is limited to only those who require access, and that access is constantly reviewed.

In recent times, underwriters have started to scrutinise the role of administrative accounts and procedures around privileged access management as a key metric in assessing cyber risk exposure.



What to Do if Your Application for a Cyber Insurance Policy is Denied

It might be the case that due to your industry sector, you may not be able to secure any cover. For many insurers, the following industry sectors are an immediate decline:



If you have been declined insurance due to poor controls, then you should get your broker to provide feedback on where to improve. Some areas can be a quick fix, whilst others may require further investment and training. Insurers are usually keen to work with clients in order to bring them up to standards.

Strengthen Your Cyber Security & Preventative Measures With ACDS

At ACDS, we provide a number of solutions to strengthen your cyber security posture. These preventative measures can reduce the likelihood of a cyber attack and potentially lower cyber insurance premiums.

Modern threats attack every element of your company and your defences should be layered to support this, in the same way as you would have multiple forms of protection for safeguarding your physical assets from intruders.

Our suite of products work across your layers of defence to enhance your protection, closing gaps left open by conventional security solutions.

Email Guard

Protects your organisation against email fraud by ensuring that your organisation is compliant with the latest standards in email encryption and authentication. This tool continuously assesses email security compliance and monitors the organisation's email authentication.

Email Guard reduces the likelihood of spoofing, which is where attackers impersonate trusted individuals or organisations. This is much harder to implement if email domain owners adopt Domain-based Message Authentication, Reporting and Conformance (DMARC), to ensure that their email addresses are not successfully used by criminals as part of their campaigns.

File Guard

Mitigates the risk of malware hidden in email attachments. Malicious attachments can lead to devastating consequences, including the deployment of malware, such as ransomware. Ransomware can be catastrophic for organisations and their suppliers, halting operations and severely impacting customer and supplier relationships.

With File Guard, employees can open documents confidently, as the original document will be removed from the email and replaced with a new copy that has been stripped of any possible malware.

Privileged Access Guard (PAG)

A workflow tool for system administrators wanting to implement Privileged Access Management (PAM). The tool grants users limited time-bound access to critical systems in an auditable manner. This limits the ability of cybercriminals to use an employee's privileged access to cause disruption.

Attack Surface Guard (ASG)

Our attack surface management tool which provides the organisation with real-time visibility into all known and unknown assets that make up your attack surface. By monitoring the attack surface, organisations can secure any vulnerabilities and weaknesses that may exist before an attacker exploits them.

Cyber Insurance FAQs

Cyber Insurance can be a complex subject; hopefully, these FAQs will answer any burning questions that you might have.

What is Cyber Insurance?

It is an insurance product that provides businesses with a combination of coverage to protect them against ransomware attacks, data breaches and other information technology-based risks.

Who Needs Cyber Insurance?

Regardless of the size of your business, if you hold a significant amount of customer data or are heavily dependent on functioning computer systems, then you should certainly consider cyber insurance.

Is Cyber Insurance Worth It?

Cyber insurance is a valuable tool for all types of businesses that want to protect themselves against the risks of cyber-attacks and data breaches. The policy will provide financial protection, legal and forensic reports as well as cover against reputational damage. Working with a good broker will ensure you get the appropriate coverage and value for money.

Who is Liable for a Data Breach?

Any business that holds personal identifiable information (PII), whether on customers or employees, is subject to national and/or international data protection legislation, which could leave them liable to regulatory fines and penalties for non-compliance in the event of a data breach.

In addition to fines and penalties for non-compliance, regulations such as the EU GDPR can also see firms risk substantial legal expenses in the event of a loss of PII.

Does Cyber Insurance Cover GDPR?

This remains a hotly debated topic within the cyber insurance market, and many consumers have accused insurers' marketing of covering 'fines and penalties', as potentially being somewhat misleading. This is certainly not the intent of insurers, and the caveat of 'where applicable by law', is always an accompaniment to any declaration of fines and penalties cover.

To date, only two countries have mandated that GDPR fines can be legally covered by insurance, Finland and Norway, with the majority of other countries remaining silent on this specific point to date, relying instead on traditional regulations around the prohibition of insuring illegal activity.

In light of recent substantial GDPR fines for the likes of Google and Meta test cases in the EU courts, this should provide a more definitive position on this point in the coming months and years.

Secure your company today and save more time and money tomorrow

Questions?
Contact us.

acdsglobal.com

hello@acdsglobal.com

+44 3302 022 033

ACDS
ADVANCED CYBER DEFENCE SYSTEMS

gaws
OF LONDON