Blackford.

Insurance Uncovered

Digital defenders: how and when to get cyber insurance

It’s easy to spot clumsy cyber crooks who try to get your details on LinkedIn or via obvious email scams. But there’s a whole world of sophisticated online criminals with a wealth of clever tools at their disposal – including customer support lines for hackers who might be having trouble deploying the malware they just purchased on the dark web. These unseen and very effective attackers are growing alarmingly quickly in numbers, ability and scale.

The UK Government estimates that almost 40% of businesses identified a cyber-attack last year. But there are likely to be many more going undetected – insurer Hiscox found that one small UK business is successfully hacked every 19 seconds.

We speak to larger businesses which have robust security systems in place, with experienced in-house teams and a board-level understanding of where cyber security fits into their overall strategy. But for one reason or another, cyber insurance isn’t yet in place.

Other organisations, which might be mid-sized SMEs, assume they’ve taken care of their risk because their IT infrastructure is outsourced to a cloud provider.

Both approaches are understandable, but even with well-developed defences in place, a properly considered cyber insurance approach can make it easier to respond and recover if attackers do manage to cause problems.

In this edition of Insurance Uncovered, we’ll outline some of the main cyber insurance issues you should be thinking about.

Why do I need cyber insurance?

The impact of being targeted by cyber criminals is a serious and growing problem for businesses all around the world. According to recent research from secure hybrid cloud experts iomart, the average business is targeted by cyber criminals twice a month. And that's the average – for companies in sectors like finance, legal and healthcare, the true picture can be nearly three times higher.

Attacks are becoming more sophisticated, better resourced, and more disruptive. From stealing personal details using clever phishing techniques, to jamming up your network with excessive traffic from automated systems, the ingenuity and determination of cyber criminals is constantly growing.

The prospect of a cyber-attack is no longer an abstract threat. It's now a matter of when, not if, your business is the target of hackers.

And consider this: while attackers can disrupt your networks, take down your team's productivity and cost you money in lost time, it can be so much worse. Quite often, hackers will use a vulnerable entry point to access a larger network and that can mean problems for your customers, clients, suppliers and other important stakeholders.

My tech infrastructure is in the cloud - doesn't that mean I'm covered?

Cloud infrastructure companies like AWS (from Amazon) and Azure (from Microsoft) have robust security in place, but no-one is impervious. That means if your data is in the cloud it's still exposed to an element of risk. Your responsibility for the safe handling of your own customers' data is no less than it would be if it was hosted on your own servers in your own premises.

Short answer – no. Cloud hosting doesn't neutralise cyber risk or shift it onto someone else. If you do it properly, however, you can reduce your risk. That's something insurers do want to see.

How do I know if my IT risk is robust enough?

That really depends. You should talk to your IT provider to make sure you've done everything you reasonably should do. The key point is to consider your specific risks and vulnerabilities and put in place measures to protect yourself as much as you can.

As ever, risk management isn't about covering every risk imaginable and installing the platinum standard mitigation across the board. It's about a sensible, realistic assessment of risk and creating a robust plan to keep your business running if things do go wrong.

The important thing is to have a plan, however. It's no longer enough to complete your Cyber Essentials certificate and implement multi-factor authentication. Cyber risk is a much more complex beast nowadays and insurers are constantly adapting their approach accordingly..

What does cyber insurance cover?

Generally speaking, there are two key elements to cyber insurance. First, an incident response service you can call on if you find yourself subject to a cyber-attack. And second, cover for your own costs in recovering from an attack or incident, as well as the expense of dealing with claims from third parties as a result of any incident.

Access to an incident response team (IRT) is a vital resource if your organisation is experiencing an attack. Many attacks are immediate, unpredictable and can be incredibly damaging if left unchecked. Depending on your insurer, notification to the IRT can be via a chat service, live call or via an app. Whichever form it takes, it's invaluable to have someone to walk you through your response, triage the solution

required and help find the right experts to support you. This may involve working alongside your own managed service provider or appointing a breach specialist to handle any data privacy claims on your behalf.

How do I get the right policy?

For something as technical as cyber security, the starting point is fairly lo-fi. The best way to identify gaps, risks and vulnerabilities is to fill out an insurance proposal.

We know that filling out a form is nobody's idea of fun. But the exercise highlights the types of questions insurers will ask, and understanding this is the best way to make the process run as smoothly as possible.

The complexity of the subject means that completing the form properly needs input from multiple stakeholders in the business (if you have a managed service provider, you'll need their help too), not just the person who normally has responsibility for insurance.

Every insurer has a different approach, different offering, and views risk in different ways, so it's important to understand which insurers are best suited to your business needs.

To find out more about the cover you purchase, or to arrange an audit of your existing policies, please get in touch.

Blackford is a trading name of Blackford Group Limited, (Firm Reference 831508).

Registered Office: Blackford Group Limited, 26 Charlotte Square, Edinburgh EH2 4ET (Registered SC616744).

Blackford Group Limited is an Appointed Representative of James Hallam Limited, authorised and regulated by the Financial Conduct Authority (Firm Reference 134435).