Not all cyber insurance is created equal

Unlike more established insurance markets, there is lots of diversity in the cyber insurance market. Policies vary widely when it comes to premium costs, extent of coverage and deductibles.

But the most concerning disparities between different underwriters and policies are the baseline compliance requirements that policy holders must meet to be eligible for receiving a payout on a claim.

Much like home insurance policies require homeowners to cover bases, such as having a sufficient amount of amperage for their circuit breakers or their swimming pools fenced off, cyber insurance policy holders are also obliged to have certain precautionary things in place.

However, the nascent cyber insurance industry has yet to agree on any sort of standard in this department, forcing each underwriter to come up with their own. On top of that, without decades of historical data to inform current policies and premiums, these underwriters are overly cautious in many cases. They don't want to overextend themselves and end up on the hook for far larger payments than they've bargained for.

So, what's covered and for how much is uncertain until digging into the details of each policy. Likewise, the firewalls, password protocols, backup processes and the like that businesses must have in place – and well documented – fluctuates wildly from one policy to the next.

Why Businesses need CDS before and after they purchase cyber insurance

Companies like CDS Office Technologies are an invaluable resource for businesses making the responsible investment in cyber insurance. They can play a key role in both making sure businesses get a good policy at a reasonable rate and ensuring they won't be denied a payout on any subsequent claims.

PREPARATION

When underwriters evaluate a potential client, they're trying to assess the risks. They want to make sure the odds are low they'll have to pay out on a claim and will calculate a more expensive premium for the same amount of coverage to mitigate the dangers posed by riskier clients.

Therefore, the safer a company's IT infrastructure appears during this process, the better the chance they'll be eligible for the coverage they seek and get a reasonable and fair rate.

If an assessor deems an opportunity too risky, they might not offer coverage at all. But if the customer seems responsible and on top of things, they're more likely to charge a lower premium and offer a policy with lower deductibles and higher payout caps.

CDS can add value at this stage by performing their own assessment and spotting the problem areas underwriters will likely flag as risks. They can then provide services and support to close weak spots in

the company's IT defenses and put in place the necessary preventative measures before they even apply.

Additionally, CDS can confer with customers during the cyber insurance process to help them evaluate their coverage options, making recommendations and steering them toward reputable providers and favorable policies.

COMPLIANCE

Once a business has signed on the dotted line and purchased a cyber insurance policy, they're expecting their claims to be paid out in the event of an applicable incident. But if they're not maintaining the "due care" expected by the insurance company, a claim could be rejected.

CDS can once again be incredibly helpful in this department by implementing any required improvements or updates on their client's behalf. Equally essential, CDS can also perform the painstakingly critical work of fully documenting and reporting on these efforts. Because even if a company has done everything right, without proof an insurance company can still deny a payout.