520.743.7554
info@computerdimensions.net
www.computerdimensions.net

6 Questions To Consider Before Purchasing Cyber Insurance

Multiple state cybersecurity agencies have set out advice for companies considering taking out insurance against hacking and ransomware attacks.

Cyber insurance can help businesses to recover after a cybersecurity attack or data breach by providing financial support to put the damage right as well as help with legal and regulatory headaches after an incident.

However, this insurance will not fix your security issues, and won't prevent a breach or attack taking place. Just as homeowners with household insurance are expected to have adequate security measures in place, businesses must continue to put measures in place to protect what they consider valuable.

Despite exponential increases in reported cyberattacks over the past year, sing-up of cyber insurance by businesses still remains low. Cyber insurance might not be right for everyone and it can never replace good security practice. If you are considering cyber insurance, here are 6 questions you should consider before moving forward:

1. What existing cybersecurity defenses do you already have in place?
2. Do you fully understand the potential impacts of a cyber incident?
3. What does the cyber-insurance policy cover (or not cover)?
4. What cybersecurity services are included in the policy, and do you need them?
5. Does the policy include support during (or after) a cybersecurity incident?
6. What must be in place to claim against (or renew) your cyber-insurance policy?

The National Cyber Security Centre (NCSC) said most insurance offered covers the immediate effects of an attack on an organization by working to quickly restore network systems and data, while seeking to minimize losses from business interruption. With data breaches there might be legal action from customers or others affected and defending or settling those claims would also normally be covered.

However, it also said potential buyers should make sure of what is excluded: for example, some insurance policies will not cover money lost through business email compromise fraud. As cyberattacks are constantly evolving all the time, companies should also check that new types of cyberattack are covered. It's also worth investigating what services the insurer provides in the immediate response to an incident to help manage recovery and improve protections and to learn what went wrong often via forensics.

Some aspects of cyber insurance are more controversial; in several cases, insurers have paid the ransoms demanded by ransomware gangs, which critics have said will encourage more attacks in the future. Insurers argue that such payouts are made at the request of their clients who are often faced with a tricky choice between paying off the criminals or a long and complicated job of restoring their computer systems or building the network again from scratch which might be far more expensive.