INSIGHTS

Cyber made simple.

one brightly cyber

CYBER INSURANCE – NECESSARY BUT HARDER TO GET

BY JAY BORDEN

The increasing frequency and effect of cyber events has driven up the financial impact on companies, making cyber insurance a necessity. Cyber insurers are well aware of the rising risks and costs and have raised rates to compensate. To state the obvious, insurance companies are for-profit enterprises very good at knowing how to assess and control their risks and financial exposure.

Two ways this is done is by refusing coverage to companies with risks deemed too high, and by increasing rates for those that have higher but acceptable risks. Even companies deemed low risk may see rate increases. The cyber event trends and the responses from the insurers combine to make it more difficult for companies to obtain cyber insurance, especially small to medium sized enterprises, SME.

But there are steps those companies, or any company, can take to mitigate their own risk and hopefully reduce cyber insurance rates.

First, know your own highest risks. Ransomware and fraud from emails, often called business email compromise, BEC, are responsible for over 80% of claims submitted to cyber insurers. In addition to the increasing frequency of ransomware attacks, the ransoms demanded are increasing.

If BEC, or emails that appear to come from an authorized party, are a major source of compromise, then using a more secure email system can help.

Many insurers consider cloud based systems such as the Google Workspace to be more secure than on premise systems. My assumption is that Google can afford higher priced talent than a company, especially a small company, to keep things secure.

CYBER INSURANCE – NECESSARY BUT HARDER TO GET

CONTINUED

Virtual Private Networks, VPN, can be a good security improvement. However, insurers follow the same thinking as for email systems. If you build or manage your own VPN you will pay a higher rate for insurance than if you use a respected VPN service.

Small and medium enterprises are better off using a managed detection and response service, MDR, rather than attempting to do cyber security on their own. They will not have the tools, talent, or experience of a good MDR service. MDR services will aim to catch penetrations before they do damage.

Cyber insurers look for MFA, Multifactor Authentication, which requires something beyond a username and password to gain access to a system or application. But remember to use phishing resistant MFA or it doesn't add much security.

As we said earlier, people are the cause of most breaches. They fall for a phishing email, click a bad link in the email, or in a text or go to a site suggested in a phone call or voicemail message. The best way to protect against this is training. It needs to be effective training and not put people to sleep. It must be taken by everyone regardless of role or level.

If a ransomware attack is successful it leaves you with two choices, pay the ransom and hope the key unlocks everything, or restore everything from backups. But that requires having current and complete backups that work.

We have written before about the necessity of good backups. Testing is the only way to know the backup works. Make sure it is good by restoring from it, determining if anything was lost, and that it is complete enough to conduct business. If you don't run a full comprehensive test you don't know if it will work. After a ransomware attack is no time to be testing your backup or finding it doesn't work. If the backup fails to get you back in business, the only other option is to pay the ransom.

According to recent research a quality tested backup made a company 2.4 times less likely to have to pay the ransom.

There is an axiom in backups called 3-2-1. Make three different backups using 2 types of media and store one off-site.

onebrightlycyber.com
(888) 773-1920

CYBER INSURANCE – NECESSARY BUT HARDER TO GET

CONTINUED

Insurers found strong backups led to claims for 72% lower damages than companies without strong backups.

Another way companies get compromised is through third parties. These can be trading partners with access to your systems or through software vendors. Both are becoming favored targets of attacker because of the multiplier effect. If a software supplier is compromised, all their customers get compromised when the software is installed. If a company with connections to many other companies is compromised, it opens the door to all their connections.

Know what protections your third-parties have in place and how well they are tested and maintained.

Not only will these techniques help keep you safer, but they will also help you obtain cyber insurance at lower rates.

Remember cybercriminals are relentless, you must be also to protect your information.

One Brightly Cyber can provide notice of compromised information 12-18 months, on average, before most other cyber services or tools. That gives you time to take the measures that render the stolen information useless to cybercriminals.

We also help you get cyber insurance at reasonable prices.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.