BLOG

The Five Things You Need to Prepare for Cyber Renewals

By Robert H. Rosenzweig, National Cyber Risk Practice Leader

Sep 28, 2021

An insurance renewal is a great moment for assessment – what you're doing well as an organization, things that are accelerating growth, coverage that is protecting your business, and areas where you may be lacking. This is especially true in the current hard market for cyber insurance. Carriers are being far more discerning and digging into controls to ensure that you're making smart, proactive decisions to prepare for potential incidents.

In advance of your next renewal, we've identified five critical measures you need to implement to navigate a challenging market and control costs while maintaining comprehensive coverage.

1. **Multifactor Authentication (MFA)**

   Historical data shows a direct correlation between cyber incidents and the lack of multifactor authentications. All users in a company, regardless of their level of access within the system, should have multifactor authentication: a sign-in method which requires users to confirm their identity through two or more separate mechanisms, such as facial recognition, a verification code sent by email or text, etc. This is especially important for remote and hybrid workforces. Someone logging in with your credentials could gain access to email, company networks, and key applications with sensitive data. If you're seeking coverage for the first time and your organization does not have MFA, for most carriers, it's going to be a non-starter.

1. **Endpoint Detection and Monitoring**

   Endpoint detection security systems monitor data in real time to determine if there are any ongoing active threats. Automatic monitoring and alert-generation is a crucial security measure, and it works best if there is a Security Operations Center staffed in-house or via a managed service provider 24 hours a day, seven days a week to monitor alerts.

1. **Security Training**

Making sure that employees undergo security awareness training is crucial. Can they recognize a suspicious email? Having up-to-date enterprise technology is great, but your employees are your first line of defense. Specialty insurance brokers can be very helpful in finding vendors that provide security awareness and phishing testing – often at a discounted rate – as well as provide analysis on the results and implement a plan to improve results. Carriers themselves often have a great deal of complimentary resources, and they want to see that you're taking advantage of them.

1. **Backups**

   Not backing up your data makes a ransomware attack exponentially more difficult to recover from – and much more expensive. All organizations should have a carefully considered process in place to restore their network with minimal disruption. This recovery plan will hinge on where your backups are being stored and whether they're being encrypted. Backups also need to be frequently tested to determine its efficacy; i.e., could it be restored within 48 hours, or is it going to take two weeks?

1. **Regular System Patching**

   Software and hardware require regular patches to reinforce any known security vulnerabilities. Ransomware evolves rapidly and is always looking for the holes that patches are designed to fill. Make sure you're staying current with your vendor's latest updates and have a regular patching cadence with immediate action taken on high priority issues. Legacy systems are those that are no longer supported by the vendor that originally offered them, meaning there will be no more patches. It's a huge exposure to keep out-of-date systems in place, especially if they're connected to other systems.

If you have any questions about how to make sure your business is set up for success during the next cyber insurance renewal period, our specialty team is always available to walk you through products, services and best practices.

We recently hosted a webinar on dicussing how to prepare for renewals. You can access the recording of that Webinar here. You can download the slide deck from the event here.

Want to learn more?

Find me on LinkedIn, here.

Connect with the Risk Strategies Cyber Risk team at cyber@risk-strategies.com.

Email me directly at rrosenzweig@risk-strategies.com.

TAGS:
Cyber