APPLYING OR RENEWING YOUR CYBER INSURANCE?

ASK THESE 20 QUESTIONS FIRST

PTG

Cyber Insurance protects one of the most important assets your company has- your data. With recent high-profile security incidents, requirements are tightening to qualify for reasonable cyber insurance premiums.

Use the questions below to prepare yourself for the questions you will encounter when applying for and renewing your cyber insurance.

- ☐ Do you perform regular backups and store them in a secure off-site location?

- ☐ Do you limit remote access to all computer systems by using two-factor authentication (not just Office 365)?

- ☐ How many PII (Personal Identifiable Information) records are held on your network?

- ☐ Do you provide periodic security training to employees?

- ☐ Do you provide security training to employees and contractors upon hire?

- ☐ Do you conduct phishing assessments? If so - how frequently?

- ☐ How do you protect privileged accounts (such as Global Administrator in Office 365 or Server Administrator accounts)

- ☐ Are processes in place to request changes to bank account details including account numbers, telephone numbers, or contact information?

- ☐ Are you using Office 365? If so, do you have MFA enabled? Do you use Advanced Threat Protection?

- ☐ Can users access email through a web application on a non-corporate device?

- ☐ Do you strictly enforce SPF (Sender Policy Framework) on incoming emails?

- ☐ Are your backups encrypted and kept separate from the network whether offline or with a cloud service?

- ☐ Do you use endpoint protection in the network? What brand?

- ☐ How long does it take you to install critical patches from your vendors?

- ☐ Do you have a SOC that is monitoring logs from systems?

- ☐ What steps are you taking to detect and prevent ransomware attacks?

- ☐ Do you allow users to have local administrator rights?

- ☐ Do you provide employees with password management software?

- ☐ Do you segment your network?

- ☐ Do you have a security baseline in place for servers, laptops, desktops, and managed mobile devices?