SmithBrothers.
Be sure.

Survive And Advance

If You Don't Have A Cyber Policy – Now Is The Time

4.15.2020

Ransomware attacks are real, and they are on the rise. With the increase in remote working, use of new technologies, distractions at home, being out of a normal routine, combined with the increase in criminal activity, you need to be asking yourself if you are vulnerable.

The criminals and hackers won't allow any room for error. Take a look at the ten questions below in order to evaluate any vulnerabilities you may have – be sure to review with your IT / security team to fill any voids and discuss other voids you may have.

Ten Questions

1. How much of the technology is the business currently using to stay up and running?
   - Taking inventory of technology platforms will facilitate creating a Business Continuity plan.
   - Inventory vendors that are critical to maintaining business e.g.. Software, IT, etc.

2. Are emails encrypted?
   - Sending any type of confidential or health information should be encrypted when sending via email. Note: a fax is now connected to the internet and is no safer than an email, unless the fax is connected via phone line.

3. Are employees using personal or company issued computers?
   - Addressing "bring you own device" in your Information security policy is critical. Non- company owned computers are more difficult to control.

4. Is the company using a VPN or cloud computing?
   - A VPN line provides an encrypted tunnel to your information. This structure is highly recommended if not cloud computing. If cloud computing, be sure to review the contract with your cloud provider on who is responsible for the data in the cloud.

5. Do you have an Information Security Policy? When was the last review and was it updated?
   - Some state laws require you have this policy in place. Depending on the carrier, some insurance policies will exclude coverage if you fail to follow your Information Security Policy.

6. Has the data backup system been tested within the last 6 months?
   - A solid backup is a great defense from ransomware, however if the backup hasn't been tested then the backup may be worthless.

7. Has the Incident Response Plan been updated?
   - If the organization has suffered a breach, the IRP is the roadmap to controlling the damage. Does it have the names and numbers of the contacts to respond? Does the response team have the same responsibilities if they are in the office or remote?

8. Is data protected at …?
   - The desktop level
   - In transit
   - At storage

9. With remote computing and the data being decentralized, is the data secured at the same level it would be if it was located within the organization's building?

10. Have your employees been trained to identify threats, report threats and educated others about threats?

Better understanding your vulnerabilities will help you make decisions about your company's package policy versus a cyber policy, as they are two different things.

- Package policies cover Property and General liability claims.
- Cyber is typically added by endorsement to the package policy with very limited wording and low limits.
- Having a separate cyber policy allows for coverage to be customized to a company's particular exposure and, is recommended, versus relying on the company's package policy.
- If you don't have a separate Cyber policy, this is the time to research and apply – not only for managing risk - but also because many of our carriers offer some gap analysis on this and some loss prevention services once you purchase coverage from them.

In our purpose of Helping Others, we are here to help your business survive during these difficult times and advance out the other end stronger. More information on Coronavirus/COVID-19 can be found HERE on our Smith Brothers Survive and Advance page. If you have questions or would like to discuss this information further, please contact your Smith Brothers risk advisor or Scott Garcia, our cybersecurity advisor. Scott's phone number is (860) 430-3330, his email is sgarcia@smithbrothersusa.com.