Lowndes

Insights

Avoiding Ransomware Attacks is Not a Pipe Dream: Actionable Steps to Avoid Becoming the Next Victim

Article
Lowndes
05.14.2021

Related Attorneys

Michael D. Piccolo

Related Expertise

Intellectual Property

Recently, the largest gasoline pipeline in the United States fell victim to a ransomware attack that caused the pipeline to go offline for several days. In addition to causing gas shortages across the Southeastern United States, it is now being reported that the Colonial Pipeline Company acquiesced to its virtual captors and paid $5 million to the hackers to stop the ransomware attack and bring the pipeline back online.

Ransomware attacks are becoming more prevalent as hackers become more sophisticated and targets continue to ignore or downplay the threat. The following are some action items that you can take today to help avoid being the next unwitting victim of a ransomware attack:

1. Buy cyber-insurance. Invest in a policy that covers ransomware, wire-fraud spoofing, and anything else your company and insurance broker think might be applicable.

2. Understand what your IT provider is actually providing you. If you outsource all or part of your IT, ask the provider to specify how the contract addresses what happens if you are breached, who is responsible for restoring the systems, notifying affected customers and employees, responding to regulators and regulatory action, defending lawsuits, who pays, what their cyber-insurance policy states, and whether you are covered (and have it written down).

3. Understand what your internal IT provides you. If you handle your own IT internally, then ask IT to show you:

    - The company's written data inventory. Maintain documentation of what data the company has, where it is kept, and how old it is. If you don't know what you have, you cannot protect it or respond in an informed way if it is stolen (or lost).

- The company's "WISP" or written information security plan. Review the plan to ensure that it covers all of the data on the inventory you just reviewed. Update it periodically, either when a material change occurs or at least yearly.

- The company's data breach response plan. Know who is doing what, how they are doing it, who to call or how all of it will work. Role play different scenarios via a tabletop exercise to make sure you have thought through the problems.

- The company's data retention plan. Determine what data you need to keep and for how long. A previous client that you haven't worked with in many years is going to be upset if you notify them that their data was stolen and is being ransomed. Old data that you are not using is only a liability, not an asset—don't be a data hoarder.

- The training plan. Create a plan for educating your employees about your data security, including what they need to be aware of, as well as what to do when there is or isn't a problem (i.e., proactive security and routine security practices).

4. Review your patch log. Regardless of internal or external IT management, ask to see your company's patch log. Confirm that it is up to date, and if it is not, be sure to put in writing a reasonable explanation and a plan for remediation with a due date. Items that are not patched for a valid reason should then be dealt with, with a "compensating control", i.e. something that compensates security-wise for the lack of patch. Failing to patch is a consistent theme in data breach.

Finally, confer with your privacy or cybersecurity attorney (or if you don't have one, think about retaining one) to ensure that you are prepared for any type of cyberattack and that you have taken the necessary precautions to prevent the cyberattack in the first place. Privacy or cybersecurity attorneys are uniquely skilled to spot critical issues, which may save you in the event of a breach.