Marketing e-Alert

How to Protect Your Business from the Next "Wanna Cry" Attack

The recent "Wanna Cry" ransomware attack that paralyzed several large organizations in the U.S. and Europe is a solemn reminder that the risk of cyber security breaches is real. Every business owner should take steps to assess the type of cyber security threats their business could be subject to and how to avoid them. The tips below are a good place to start:

- **Don't underestimate the risks.** Many small business owners are too busy taking care of day-to-day responsibilities to keep cyber security top of mind. This is a mistake—the greatest weapon against attacks is awareness and having a plan in place to prevent them. Reinforce prevention by incorporating a plan into employee onboarding and offering ongoing training.

- **Make updating software a priority process.** As the "Wanna Cry" attack taught us, updating your computer software is an essential prevention strategy. Many of the infected computers at large organizations were not updated—leaving entire networks vulnerable when just a single computer was compromised. A regular schedule and protocols for updating software can help mitigate cyber security risks.

- **Learn the signs of an attack and what to do about them.** The most effective way to avoid falling victim to another Wanna Cry-like attack is to be aware of the type of emails that may contain ransomware or other viruses. These emails typically include an attachment (often a .zip file) that you didn't ask for, and may come disguised as an email from someone you know. If in doubt, the best course of action is to delete the email immediately.

With the risk of cyber attacks growing by the day, it's time to take action to protect your business. Educating your employees is key, as is updating your software on a regular basis. You may also want to ask an IT professional to help you evaluate and mitigate risk in this area.