APRIL 2015

South Florida Hospital News® and Healthcare Report

THE REGION'S MONTHLY NEWSPAPER FOR HEALTHCARE PROFESSIONALS & PHYSICIANS

Don't Let Cybercrime Bankrupt Your Business

BY MICHAEL CURTO, CPA

While there is no doubt that technology makes people's lives easier, it also provides a way for criminals to take advantage of all of the information that is stored on computers, phones, tablets and business IT systems. In addition to the loss of financial assets, cyber criminals can also steal intellectual property, damage a company's brand and reputation, cause disruptions in a business's online presence, and result in legal liability when customers' online information is stolen.

A 2013 report prepared for McAfee estimates that cybercrime results in a loss of between $24 billion and $120 billion in the U.S. each year. And it's not just large corporations that are targeted by cyber predators. In a report by cybersecurity firm Symantec, small businesses with fewer than 250 employees represented 31 percent of all attacks in 2012, up from 18 percent in the prior year. ClikCloud estimates that the average cost of a data breach is roughly $6.75 million, or $214 per compromised customer record—which could bankrupt some businesses.

Even as new technologies are created to battle these attacks, cyber criminals are working just as hard to find ways around them. No matter how well engineered, every network is susceptible. Imagine how your practice or hospital system would fare if hackers were able to access patients' medical records and personal information, steal research results, or circumvent your network to read unencrypted data. For this reason, it is critical to be vigilant and to repeatedly verify that countermeasures are in place and working properly to keep in compliance with HIPPA regulations.

There are things that you can do to protect your business from the threat of cybercrime. These include:

- Creating a comprehensive policy to deal with attacks
- Undergoing an IT risk assessment and audit
- Creating a data breach response plan
- Having employees undergo security awareness training
- Reviewing security operations and architecture design
- Undergoing attack simulations to determine vulnerabilities

Taking a proactive approach to protecting your business from hacking, corporate espionage and malicious destruction can save you time, money and a myriad of other problems, including issues with regulatory compliance. Let Marcum help you identify, assess and remediate vulnerabilities in your IT environment.

For additional information, contact Michael Curto at Michael.Curto@marcumllp.com or (954) 320-8000.