OP Cloud and On-Premise Information Security

Last Modified on 09/20/2023 9:07 am EDT

There is no shortage of news stories about businesses, educational institutions and governments that have been affected by cybercrime.

Do not think that your practice is too small or uninteresting to be a victim. Attackers target all types of businesses, but healthcare is particularly attractive due to the amount of personal information available and its value to criminal organizations.

In addition to the monetary and reputational losses you can experience from a cybercrime incident, there may be HIPAA or other regulatory penalties which will add to the recovery efforts and costs. Estimates suggest that 60% of small businesses that experience a cybercrime incident go out of business within six months.

According to the CISA 2022 Risk and Vulnerability Assessments report, more than 85% of all intrusions begin with phishing or other forms of credential misuse. So, protecting your user accounts and passwords should be a top priority.

Your first line of defense in stopping phishing and malware is your staff. All practice staff should be trained to identify phishing attempts and to alert the appropriate group should any information be accessed by unauthorized parties.

In addition to general information security knowledge, all practice staff should be familiar with HIPAA rules and any other applicable regulations for your location. You should perform periodic reviews and assessments of the staff's understanding of these regulations. Like phishing, staff should alert the appropriate group should any information be disclosed to unauthorized parties.

For additional information about OP Cloud Information Security

For additional information about On-Premises Information Security