NCSAM is Over. Focus on HealthIT Security is Not.

October has come and gone and so has yet another National Cybersecurity Awareness Month (NCSAM). But this collective effort between government and industry to make us all safer online didn't end on the 31st.

Almost $8 million dollars. That's the average US cost to mitigate and resolve a data breach, according to a recent study by the Ponemon Institute. And the healthcare industry's breach costs are higher than any other industry, at an average $408 per record. With numbers like these, it's not surprising that cybersecurity is on the minds of health IT executives. To improve your organization's cybersecurity, make sure you're following these data security best practices.

Have a Proactive Plan. The old cliché of "if you fail to plan, you plan to fail" holds true when it comes to healthcare cybersecurity. Develop your unique breach response plan before any such breach occurs by identifying the appropriate actions for mitigating the breach situation and keeping stakeholders informed.

Mobile Convenience vs. Mobile Risks. Risks are real when it comes to the increased usage of tablets and smartphones in the healthcare environment both on the provider and patient side. It is imperative that IT decision makers implement mobile device management (MDM) in their planning. MDM will allow you to administer, secure and enforce policies on phone, tablets and other mobile endpoints.

Knowledge is Power. Empowering your employees with security knowledge creates a front line of defense against data breaches and other cybersecurity issues. Providing best practices training for current and new employees to teach

optimal ways to handle sensitive data can present a united front against malicious hackers.

Seamless Upgrades. Hardware and software upgrades and patches need to be acted on immediately in order to avoid unnecessary risk. For best results, create and execute an update plan that includes all elements of your system, from mobile devices to Internet-connected healthcare equipment.

Limit Physical Access. When you think of a hacker, you likely think of someone gaining unauthorized access to your system via electronic means—like through an unpatched vulnerability in your network software. And while many times this is the case, the reality is that hacking and cybersecurity issues can and do occur when a malicious person gains physical access to your systems. A stolen laptop or damaged server can be just as dangerous as a network vulnerability when it comes to cybersecurity, so ensure that you control access to areas containing highly sensitive equipment.

Not If, But When. Today, the question for healthcare organizations is not if you will be the target of a breach but when. And by following data security best practices—like creating a response plan that includes mobile devices, training employees, quickly applying updates and patches and keeping physical control of access to your network—you'll be on your way toward improving your organization's cybersecurity.

To learn more about NCSAM and resources available to you and your organization, visit staysafeonline.org/ncsam/.