How to build a secure cybersecurity dashboard

The protection of patient data is of paramount importance to health systems. One way to achieve this is to have cybersecurity dashboards, which serve as tools to stop breaches before they happen and squash threats that manage to slip past their safeguards.

While the components of a successful dashboard are largely dependent on the needs of an organisation, there are a few characteristics common to the most effective approaches.

Here's a checklist of some important things CFOs need to consider when building a cybersecurity dashboard:

• Password security is a must. Ensuring good password practices is the first line of defence against potential hackers. Make sure all of the endpoints in the system – every computer, MRI machine, mobile device and electronic health record – are protected by strong passwords. The passwords should be encrypted, contain letters and symbols, be a minimum 8 characters in length, and be available on every system at the hospital.

• When all of the endpoints are successfully connected to the system, make sure your dashboards give you visibility over all of them. You will know who has strong passwords, who needs to make changes, what they logged into and where. Importantly, if there's a breach at one of those terminals, you and your team should know instantly.

• It will likely take multiple dashboards to get the coverage you need. Don't worry about it – it's usually just a matter of having a few different tabs open. All the dashboard information is right there across the tabs, so it's not too difficult to consume.

• Invest in remediation software. An ounce of prevention is worth a pound of cure, but safeguards aren't perfect, so have a cure ready. The good news is that remediation software is relatively simple and inexpensive to implement.

• Run tests often. Make sure your employees aren't susceptible to phishing emails, and consider annual SOC audits. Standing for System and Organisation Controls, SOC audits cover the protocols of an organisation and how it protects information and patient data.

• Dashboards should be customisable and adaptable. They should display what's important to the person running the project.

• Have failover systems. Redundancy will only get more important as IoT advances.

• Dashboards should allow for transparency between management and the IT team.

Source: Healthcare Finance
Image Credit: iStock

Published on : Wed, 31 Oct 2018