BioSpectrum the business of Bio & Health Sciences ASIA EDITION

Future of security in healthcare

04 August 2015 | News | By BioSpectrum Bureau

Future of security in healthcare

Singapore: According to the global consulting firm Tower Watson, Singapore has one of the most successful healthcare systems in the world, in terms of both efficiency in financing and the results achieved in community health outcomes.

The success of Singapore's healthcare system can mostly be attributed to connected healthcare that has been implemented across the providers. Through the connected healthcare system, patients have the ability to enjoy technologies that provide healthcare remotely. Most importantly, connected healthcare also allows consolidating medical record of a single patient across different hospitals. When integrated, record would allow patient data to be consolidated quickly and accurately. Locally, Singapore's National Electronic Health Record (NEHR), launched in 2013, will lead to just one single health record for one patient. The tagging of the patient's prognosis, treatments and allergies at different medical centers will be at one single area virtually.

The rise of patient's involvement and engagement in their own health, as well as the increased use of electronic health record

urge healthcare organizations to reinforce and modernize their IT infrastructures. As healthcare organizations adopt new technologies to enhance the quality and efficiency of the care they deliver, they must also reassess information security policies.

Here are the key steps to follow to ensure the healthcare organizations' network remain secure despite the growing number of applications and mobile devices connected to the network.

Understanding the risk

The use of mobile devices through connected healthcare system brings security challenges along with the necessity to enable seamless access for both doctors and patients. The wireless LAN in hospitals is getting saturated with data and devices as clinicians use laptops and tablets to view and enter patient data. Yet, unrestricted usage could jeopardize patient privacy as well as place an unprecedented burden on the network and IT resources.

Because of this, today's healthcare organizations are at greater risk of cyber-attacks than ever before. A recent report from IDC stated that cyber-attacks against healthcare will assuredly increase in number and level of sophistication in the next 12 to 24 months . This urges healthcare organizations to take a more proactive stance in protecting themselves by improving security of mobile applications.

Getting prepared

Because the risks are here, healthcare organizations have to face this reality and implement the right policy. It starts with undertaking a current-state assessment of the data the healthcare organization owns, manages and uses. Before taking further concrete action, the IT team must take stock of everything - in terms of both technology and information - the healthcare organizations handle.

IT team should also undertake a formal review of the organization's current security policies to identify potential threats. This means identifying all the risks to electronic health information that the organization faces, trying to understand the likelihood of an undesirable action or event occurring as a result of that risk, and evaluating the impact of such an action or event on the organization or its patients. Only then can the IT team develop a formal security policy to define the roles, responsibilities, acceptable use, and security practices.

Among large healthcare institutions and hospitals, executive-level roles, even departments, are being created that are dedicated to fulfil this sole need of defending the data and combating these threats. It is driving the future of security in healthcare. Some examples of these dedicated roles include the Chief Information Security Officer, Director of IT Governance, and Director of Information Risk and Compliance.

Organizations should also look at educating employees about security issues. Awareness and training activities related to security need to be reinforced to empower every employee to acknowledge that security is critical to the stability of the organizations they work for and to ensure they quickly recognize the signs that something is wrong in the network.

Improving approach to protection

The network has become an intrinsic and essential component of the IT infrastructure. Almost all enterprise applications and, thus, business processes are supported by the enterprise network . A life-critical wireless healthcare network, therefore, needs to provide the correct architecture that is continuously available, pervasive in a cost-effective way and secure at any time. This includes the ability to provide the healthcare institution of today with a technology infrastructure that is flexible, secure and scalable, while decreasing liability risk. Due to economic considerations that healthcare faces today, it also needs to demonstrate the best Total Cost of Ownership (TCO).

There are now converged wired/wireless network architectures that offer significant value to today's healthcare organizations and limit the risk of breaches. These architectures can simplify the overall management of the network and allow for the assignment of single user or device specific configurations regarding traffic segregation, QoS and forwarding. These policy-based architectures also keep traffic from all different services segregated and isolated. Having a policy-based design and isolation of traffic will enable healthcare organizations to address different medical device application requirements and the rush to BYOD in healthcare, while ensuring security of the network.

The world of healthcare IT is continuing to evolve at a rapid pace and it is critical for today's healthcare organizations to implement the proper infrastructure in order to successfully deploy and support cutting-edge, digitally-enabled tools, wearables and mobile applications. At the same time, the transmission of all data between computer equipment in hospitals

must be reliable and secure, without any outages or risk of the information being accessed by unauthorized parties. Healthcare cyber security strategies, therefore, need to take a comprehensive approach and include not only react-and-defend capabilities, but also predict-and-prevent capabilities to effectively ensure security of the network.