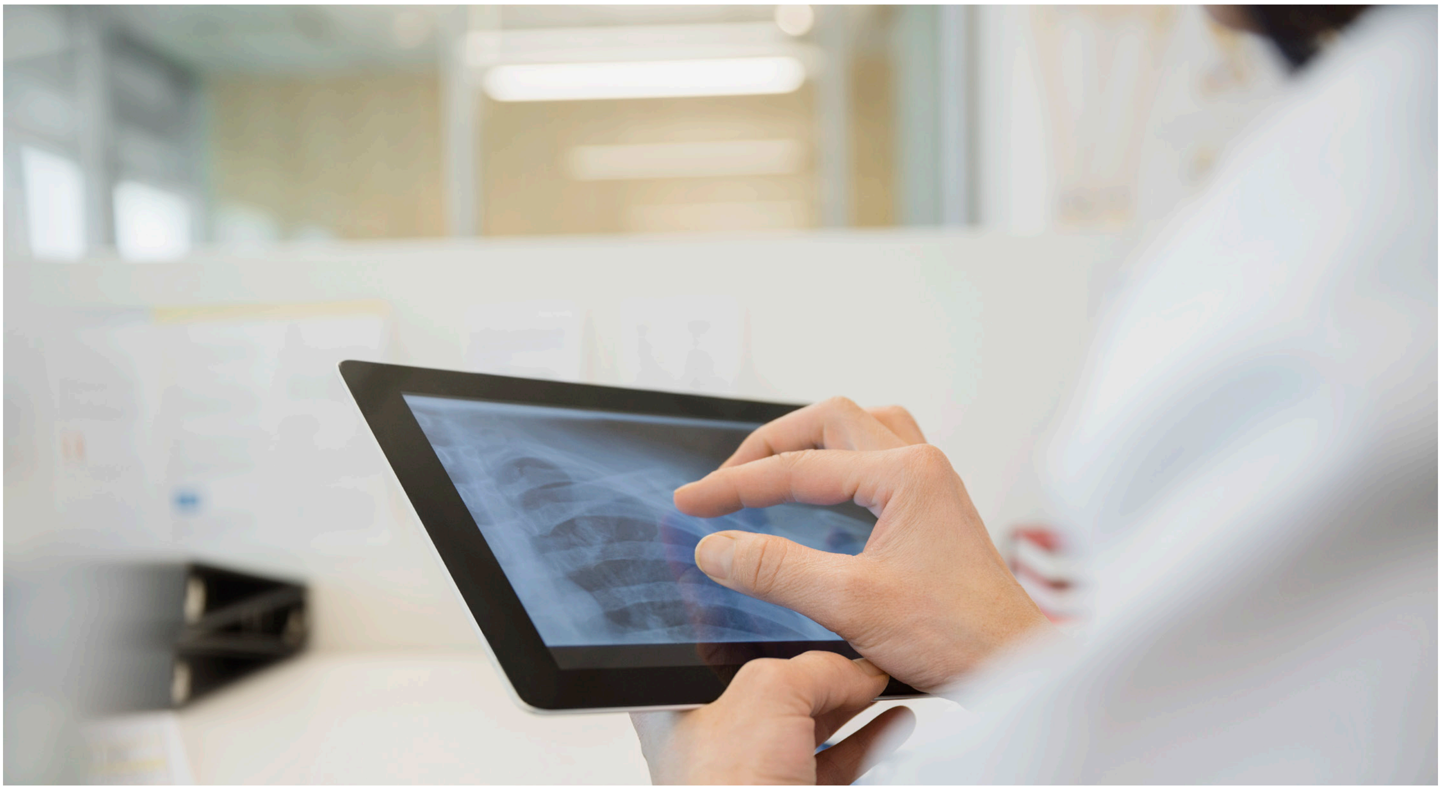
Factsheet

Healthcare Provider Consulting Solutions

Small Hospitals Can Afford Big Cyber Security

written by Daniel Stewart, Vice President IT Strategy and Cyber Security

Today, healthcare data breaches and ransomware threats are growing at an exponential rate; over 90% of healthcare organizations have reported a data breach in the last 24 months. Investing in cyber security programs to mitigate the risk of these attacks has become a major priority for hospitals of all sizes, but to date, more often than not, the smaller provider facilities have not had the same level of focus in this area as the larger hospitals and health systems.



Trusted partner for your **Digital Journey**

The community and small rural hospital market segment has the same cyber security needs and risks as bigger facilities but a much more difficult time prioritizing this with all of its other capital and operating dollar requirements. Most providers in this space are running on razor thin margins already so to determine the level of security that is affordable and provides the appropriate protection against hackers is a huge challenge. However, implementing an effective cyber security program is no longer an option, failure to do so can jeopardize the continued success and even survival of these small hospitals.

As the industry continues to move toward value-based care, with the accelerating growth of access points, and the collection of more patient-centric data, smaller hospitals are increasingly vulnerable to cyber-attacks. One reason is that many are only focusing once per year on reviewing their policies and procedures for HIPAA security compliance and believing that this provides adequate protection. This is certainly one component of a Cyber Security program but alone will do little to mitigate the risk of an attack.

In order for a small hospital to develop and maintain an affordable Cyber security program that will protect its vital assets and reputation, the specific threat matrix of the organization must be understood. Based on that matrix the appropriate mix of security solutions can be developed.

For a small hospital, typically the best and most affordable approach is to initially bring in a qualified third party to assess its current environment and work in conjunction with hospital staff to develop and execute a remediation plan specifically based on its threat level.

Listed below are 5 steps that must be completed in order to evaluate the current status of cyber security and develop and maintain an appropriate and affordable Cyber Security Program across the organization:

1

Understand the environment and specific threat matrix through an ongoing assessment process. This enables the hospital to only include necessary services and not spend dollars on security measures that provide little value

2

Focus on the basics in developing a remediation plan:

- Improve data security policies and procedures and establish evidence of compliance
- Develop a formal governance structure as part of documented procedures to create an internal security team to monitor and manage data security policies, procedures and required remediation. For a small hospital the likelihood of bringing in, affording and retaining a CISO and/or other security personnel is very low
- Implement and maintain industry standard cybersecurity practices such as regular system patching and testing of firewalls and other systems
- Move to next Generation Virus software that is script based vs definition based. This will improve desktop security

3

Consider partnering with a qualified 3rd party that can work with the internal team on the initial assessment and can conduct periodic security reviews including penetration testing and mock phishing attacks. The evaluation of an outsourced arrangement where a third party manages selected on-going security services on a remote basis may be another alternative. Again this approach in many cases can be the least costly and most efficient ongoing support option for a small hospital

4

Formal and continuing staff education is critical. The weakest link within any organization is its people. Even the most advanced technical safeguards can be intentionally or unintentionally thwarted by people

5

Finally, as part of the overall security program develop and put in place an incident response program that is linked to the Hospital Incident Command Structure (HICS). This educates internal stakeholders on how to react to a breach, roles and responsibilities, what to say to the media, and things to consider in terms of liability insurance, etc.