STEPS TO PROTECT YOUR ORGANIZATION FROM CYBER RISK AND MAINTAIN NETWORK SECURITY

Posted on March 18, 2020 by Kristian Cruz

Categories: Healthcare IT, Uncategorized

There are many steps an organization must follow to maintain network security, the first and most important starts with the decisions of the company executives. It is their responsibility to set the standard for their organization's non-physical and physical security controls. Excuses such as; the firm is too small, IT should manage it, network security is too complicated, and an inflexible budge can directly lead to a compromised network. Management can even create an environment where IT leaders will assimilate into this faulty attitude. Once that happens, the negligent attitude towards cyber liabilities will eventually result in a severe consequence — network breach. This is even more likely for companies in the healthcare sector; see blog, "Healthcare Rates Worst of Eight Sectors Most Likely to Be Breached."

Here are some recommendations for Healthcare organizations to follow to be better prepared and protected...

1. **Be inquisitive**
   - Start asking your team questions that can help you develop a plan. Begin by understanding what recommendations your team has and how long it will take to implement them. Then, ask for an estimate of how much it will cost. Ask if and how these changes will produce a return on investment through fewer issues, better performance, and a refined operational maturity. If not done so already, ask your team to assess the financial and cyber risks, as well as regulatory costs, in the case of a serious or minor breach. Try to create a meaningful conversation with your team in order to be the most efficient. If you're having trouble getting answers and creating an efficient conversation, then you should question if your cybersecurity and IT operations are being managed by the correct people.
2. **Conduct a comprehensive review of your company's budget**
   - Once you've asked your team all the questions needed, your next step should be forming a budget to include the new IT security needs. It's important to note that security is a very broad category and it will most likely branch out to many specific things. Also, developing

a budget to include the extra security costs is more of a long-term plan rather than a short-term one.

3. **Change the negligent attitude towards cybersecurity and privacy**
    - Make sure to keep asking questions during your process of becoming more operationally mature with cybersecurity. Remember, the first step of network security begins with the decisions of the company executives. Once management notices that the leaders of an organization are taking cybersecurity more seriously, they will then shift towards having the same attitude of protecting the company, maintaining patient privacy, and increasing profitability for shareholders.