iatricSystems Shares How Cybersecurity Tools and Resources Can Work Together

Guy McAllister
Director Privacy & Security,
CISA 405 (d) Task Force Member,
Board Secretary/Treasurer of
Community Health IT

iatricSystems™, Inc.

How would you rank provider organizations' sophistication levels in being able to properly defend themselves against cyberattacks (1 to 10 scale with 1 being completely unprepared and 10 being extremely advanced in their preparation)?

The level of sophistication related to defending against a cyberattack varies greatly. Smaller provider organizations may struggle to dedicate financial and human resource investments to protect against cyber threats. Larger health systems may be more advantaged with dedicated resources. As a result, I would say on average our industry is a 6, trending upward – often by necessity not choice.

What core challenges remain that are holding organizations back from having more advanced and proactive defense strategies?

One of the core challenges holding organizations back is threats being numerous and ever changing. There is no one-size-fits-all solution to "fix" the problem of defending against attacks. A key area of vulnerability is remote access in healthcare. While allowing vendors and employees to access hospital networks is a critical part of our daily operations, it remains a challenge. In many organizations, the method of remote access is cobbled together tools attempting to allow access to the network. Therefore, the ability to detect and prevent threats is sometimes non-existent. Remote access monitoring and management must be part of the sophistication of cybersecurity preparedness. Organizations need to employ multiple tools to defend against multiple types of threats.

What cybersecurity best practices would you recommend above all in this current moment and how can technology/IT tools further help in this area?

Above all, multi-factor authentication is a must to protect your network from the growing threat of third-party breaches, especially on external access, but preferably for all access. Invest in both dedicated resources and cybersecurity tools, then train the people and use the tools. Let tools, like AI work for you to determine behavioral activity and define what is normal and what isn't. Using technology first will make your audit managers more effective and efficient. These solutions are a must where ePHI is concerned. Monitoring network access without monitoring ePHI access is dangerous and unwise.

Do you feel that cybersecurity professionals are currently empowered enough to drive change throughout their organizations?

I believe that the empowerment is evolving. Driving change in many healthcare systems involves physicians and senior leaders (especially CEOs). When I was a CIO, clinicians viewed EMRs as a workday disruptor. Similarly, today, cybersecurity initiatives are often viewed as disruptive by clinical care providers because the initiatives involve additional steps and thus viewed as inconvenient. Those organizations that start seeing cybersecurity as a way to protect their patients and their organization versus as an inconvenience will have the empowerment. If the CEO recognizes the pain points of a cyberattack or breach, then cybersecurity professionals in that organization will be empowered to secure and protect. But, if the perceived inconvenience of security stirs the special interest groups and the CEO acquiesces, then cybersecurity professionals in that organization will ultimately fail to secure and protect.

Another concern senior leaders may have is the required IT cybersecurity spend. After the latest round of EMR replacements and upgrades, cybersecurity may not be at the top of the list for spending. But remember, the cost of recovering from a breach far outweighs investments in cybersecurity protection up front (both in monetary and in reputation).

How do you foresee the next 12 to 24 months playing out in the healthcare cybersecurity landscape? Do you think things will get worse before they get better or do you have a more optimistic view?

I agree with CHIME policy experts, who recently said, "A number of health IT-related bills, including those focusing on telehealth and cybersecurity, are expected to be introduced by lawmakers next year, but they will likely be stalled in Congress with the upcoming election and the impeachment inquiry…" In the next 12 to 24 months, as consumer frustrations continue to grow over privacy breaches and as ransomware attacks continue to increase and impact our organizations, pressure for Federal regulations will increase and how well an organization is or is not securing and protecting its data will become more transparent. Intentionality in healthcare cybersecurity will need to step up and improve in the next 12 to 24 months. Patients (consumers) will demand it.