Cybersecurity Risks and Challenges

Ron Ropp, CISSP
CTO & CISO
HealthITq

Dr. Robecca Quammen, FACHE
CEO
HealthITq

How does the overall nationwide U.S. healthcare system landscape around cybersecurity look like to you right now?

With extensive experience in numerous healthcare entities, our collective experience is somewhat jaded. Sometimes I feel as if the industry has just become numb to the inevitability of a cyber attack of some kind and resigned to accept it as it comes. Of course, there are many in the trenches who take it very seriously and work tirelessly within the confines of their respective administrative and financial support to safeguard the environments in their charge.

The "haves" and "have nots" – large, well funded healthcare systems generally have appropriate teams, infrastructure, and protections in place. Clinics and smaller to mid-size and independent systems frequently do not. But as we have come to expect, even those who are better prepared, in text book terms, to thwart cyber activity, offer significantly more opportunity as desirable targets.

Do you see the threat vectors as having intensified recently?

Yes - they have always been there, but visibility and frequency have increased. The visibility is a good thing but organizational response continues to lag behind threats. There are attempts to share information but that effort remains fractured, nonstandard, and inconsistent. Major HHS alerts occur, but are frequently discounted at the ground level. Cybersecurity vendors drive the narrative with sponsorship and adequate funding rarely achieved until an attack occurs or insurance liability carriers force preventive action such as their recent hard-line requirements for MFA.

What about the threat posed by state actors—e.g., foreign governments—becoming involved in purely destructive (non-remunerative) cyberattacks, such as DDOS attacks, against healthcare organizations in the US? How can provider leaders prepare?

The answer is simple - get ahead of it instead of reacting to it. It is not enough to hire cybersecurity leadership in organizations, the hardest part is listening to them and taking action when they indicate it is necessary. Cybersecurity is like going to the gym - everyone talks about it, but a very small number do it consistently. Have good plans and test them. Staff cannot wait to gain approvals to mitigate a threat at 2am so plans must allow for immediate and independent decision making.

How quickly are health IT leaders "suiting up" in terms of hiring CISOs and giving those CISOs the staffing and the funding needed to be effective?

There are visible efforts throughout the industry, but the CISO and CIO in many organizations still do not have significant voice within the executive leadership function. Many organizations are simply checking the box when it comes to hiring a CISO without providing the needed budget, authority, team, or presence at the C-suite and Board levels.

With many competing initiatives vying for scarce healthcare budget dollars, cyber security funding consistently suffers as it is not revenue generating, is not well understood, and falls in the category of *it must not be a serious problem since we have not experienced an attack.*

How quickly are patient care organization leaders adopting advanced strategies, including behavioral monitoring, auditing of backups, advanced network segmentation, and the engagement of SOCs (security operations centers)?

Not fast enough, and even when adopting them, putting the hands behind the tools is challenging. A good SOC team that understands healthcare is rare among emerging vendors. And building an in-house team is a challenging endeavor that takes time and money.

What kinds of upgraded capabilities must the vendor community as a whole be prepared to offer patient care organizations?

Learn healthcare as a vertical. Most vendors say they know healthcare, and yet their teams have not experienced healthcare operations. Understanding clinical and financial workflows along with patient and physician impact, remains one of the biggest challenges for software and cyber solution vendors.

What do the next few years look like in this key area?

Healthcare is a soft target for bad actors. Vendor partners and leaders who make this a priority in their organizations will be the most successful. The cost for an organization to maintain cyber health is staggering, so a commitment to funding and personnel is key. Technology exists and improves daily - but knowledgeable staff and executive commitment still represents the strongest organizational allies against cyber activity.