Managing Cybersecurity + Risk in Rural Hospitals
In recent years, health care organizations have made tremendous progress in the digitization of health care information and workflow. Significant benefits have been achieved and more will be realized as systems and processes are optimized. However, with all of its benefits, digital health care has also introduced new threats and vulnerabilities. Among those are cybersecurity threats and risks, which include the theft of records through hacking and cybercrime, as well as through insiders, and medical device vulnerabilities and risks related to breach reporting requirements. Hospitals can prepare for and manage such risks by integrating cybersecurity preparedness into their existing governance, risk management and business continuity framework. This dialogue will explore what rural health care organizations are doing to improve cybersecurity preparedness.
MARK HERZOG (Holy Family Memorial): The security of the information that we use, because it is so vital to our organization, is of paramount importance to us. We have a deep strategy relative to information services going back 15 years. We haven’t experienced a breach, but we had a close call. A laptop was taken from one of our storerooms. Fortunately, it did not include patient information, but it was an eye-opener. We outsource our IT department, so we have access to expertise that we may otherwise be unable to find in our community.

KATHY LANDRETH (Bath Community Hospital): I’ve been at Bath Community Hospital for two years. We are a 25-bed critical access hospital in a Virginia resort town. Previously, I worked in a large health system. When I started, cybersecurity was low on the list of priorities. There were a lot of things that weren’t being done. It has been elevated as a priority, but there is still work to be done. Our board education for cybersecurity has been hit or miss. It hasn’t been a significant focus. But then we had an incident that raised awareness and
increased the need for prioritization. We often think of cybersecurity as a breach in patient information, but it's much more than that. Ours was essentially an email scam. Our chief financial officer received an email that appeared to be from me asking him to wire money to a third-party vendor. When he didn't do it right away, he received a second email. When I saw him the next day, he informed me that he took care of the wire transfer. Of course, I asked what he was talking about. And he told me about the emails. The scammers were able to penetrate our system and replicate my email. Fortunately, this was a near-miss because our bank was suspicious about the transaction and did not transfer the funds.

Afterward, we spoke to our IT person. She pointed out that I typically make these types of requests in person and not via email. But, of course, we are all busy. So, we reviewed the process to see what systems we have in place to keep this from happening and looked at the security of patient information. We educated all of our managers at that time about the things that we were doing and warned them about suspicious emails. We have really beefed up our efforts. It's hard because our IT staff consists of one person. Going forward, we plan to focus on board education and continue to review our policies and procedures. We have a committee chaired by our IT person, and we will review our policies and procedures annually.

JEFF BELL (CareTech Solutions): The annual review process is important. When you look at your policies, you’ll likely find references to technology that you don’t use anymore, like BlackBerrys.

LANDRETH: Yes, or people who are no longer at the organization who are named in the policies. It's a challenge for small hospitals.

MARC AUGSBURGER (Caro Community Hospital): We are also a 25-bed critical access hospital. Over the past two years, we've hired a third-party organization to conduct a risk assessment. We also participate in the Thumb Rural Health Network which consists of hospitals and health departments in east central Michigan. We meet as a group monthly. A year ago, we purchased a PC and the software that all of our facilities could pass around to do intermittent security testing, as well. This is in addition to what the third-party vendor is doing. We get the PC once or twice a year in addition to the full-blown testing that we do.

We have not had any incidents to date, which is fortunate. But we still need to be cautious. We didn’t have a policy in place until two years ago and we’ve worked hard to educate our employees. But it’s something we need to keep focused on because people forget and get busy with other things. We’ve sent out test emails to assess our vulnerability, asking our employees to respond with data that they should not provide. The first results were pretty dismal. Sixty-percent of our employees failed. I’m not comfortable with that number. But it gave us the opportunity go back and
re-educate our staff. Now we put something about cybersecurity in our monthly email newsletter to remind them of specific things that they shouldn’t be doing. We’ve certainly tried to step it up a notch. And now our staffers call IT — we had a three-person IT staff — to ask questions. It has raised awareness now that we’ve started to test our employees.

KEVIN STANSBURY (Lincoln Community Hospital): We’re a 15-bed critical access hospital in rural Colorado, about 70 miles in any direction to the nearest hospital. Last summer, we did have a cyberattack. It started with a lot of strange activity. I received emails from a law firm in Los Angeles saying they represented us in an IRS matter and they wanted me to proof a document they were going to send to the IRS. That same week, we got a number of emails in our finance department that asked that invoices be paid. The emails were increasingly aggressive. We didn’t recognize most of the vendors but, for those we did recognize, the invoice was not in line with how we’d done business with them in the past.

We found the source of the break. We had a laptop being used by a provider. She had taken it home to do some charting and the laptop was infected on her private network, and then she brought it back into the hospital. It shut down all of our applications and functionality on our electronic health record. We didn’t have any patient data access; we were down for several days in terms of operation on our EHR. Also at that time in our area, several other rural hospitals in eastern Colorado experienced a similar attack.

During that period, we had only one IT person, which is not atypical. We’ve since beefed up our staff. We’ve brought in a chief information officer, for example, along with another tech person to kind of “fix and do.” We have worked, as others here mentioned, to review our policies and procedures. We conduct an annual vulnerability assessment. We did fairly well — 80 percent of our employees passed — but it was close to our breach. We do have cyber insurance, but it wasn’t particularly effective, because it reimbursed very few of the expenses that we incurred.

One of our challenges is how we balance security against functionality. We don’t want to make it too difficult for physicians to access the EHR.

STEVE TENHOUSE (Kirby Medical Center): Kirby Medical Center is a 16-bed critical access hospital with a fairly robust IT department. We have four people in our IT department and two more in informatics. We do conduct an annual risk assessment to understand our vulnerabilities. We are a member of the Illinois Critical Access Hospital
Network, which provides IT services that will conduct penetration testing from a number of different outlets. About six months ago, we had a debate about whether to keep our EHR system and all of our internal network files within the hospital on our own server system. We decided to move our EHR and some of our files off-site to a server farm. One of our concerns was whether being part of a bigger network made us a bigger target. We had a lot of discussion. Is this better? Is this worse? We were pretty low on the radar screen when we were by ourselves on the network. Obviously, if we’re part of a server farm, we are potentially part of a much bigger target. Ultimately, we decided to move to a third-party server.

It’s interesting. The low-tech attacks are the ones that get you. We had a similar experience to what Kathy described. It happened a year ago. I was on vacation and did not have access to cell service so no one could reach me. When I finally got cell service, I had several messages from my controller telling me that she was able to get the $15,000 wire transfer payment made. When I called her, she said, ‘You know, it took some doing, but I got your emails and I was able to process the payment.” When I told her I hadn’t sent any emails, she fell silent. She had received several emails that morning that appeared to be from me. They had added another ‘r’ to Kirby, but on quick glance, it looked like my address. We have since changed our email system; any email that comes from outside the organization has an ‘EXT’ prefix in the subject line. Anyway, all of the processes that we had in place to prevent such an occurrence did not work as they should have. The controller went to the local bank — we’ve done business with them for 30 years — and told them that I was away and needed to have this done. The bank did try to call me. But then they decided to process the transfer without speaking with me. We pushed back with the bank because it broke policy. Our bank said it reached out to the other bank, which agreed to return the money. When staff don’t follow procedure, you open yourself up for potential risk.
MODERATOR: How are you educating your boards about the risk potential? When something happens, how are they responding?

HERZOG: There is greater opportunity for us to engage the board around this issue. Our board has direct interaction with our IT company, but we know we need to enhance our board education. We do have cybersecurity coverage, that includes a review of our procedures by the insurance company. It gives us an additional set of eyes to assess our risks.

STANSBURY: We reported our experience to the board members right away. We had been talking with them about the need to update our IT systems, so it was on their minds. Obviously, we received a lot of support to fix what we needed to fix and to make the necessary investments to enhance security. Earlier in the year, when we’re discussing capital priorities, we discussed our vulnerabilities. We felt we were a bit vulnerable even though we are a small organization, under the radar. But when we are talking about private patient information, that’s a risk we don’t want to take. We purchased additional insurance and provided board education. We’re members of the Colorado Hospital Association, and it has provided education on the topic. We’re focused on security and our board is supportive.

AUGSBERGER: Our board has been supportive as well. We review the annual third-party report with the board, ensuring full transparency. We highlight our strengths and potential weaknesses. We’ve also purchased additional insurance. It’s expensive, though.

STANSBURY: It is expensive, and didn’t cover everything that we hoped it would. It did cover overtime that was needed to reconstruct the reconfiguration on the servers, and some other expenses. But it didn’t cover some preventive measures because they deemed it was something we were planning to purchase anyway. I talked with our risk manager about whether the insurance was worth the cost. We determined that it was, and it paid off for us. We have since moved to a third-party storage vendor because they understand the threats that exist.

BELL: That makes a great deal of sense for small organizations. The third-party vendors have dedicated staff that are focused on the issue. They are operating at a level of secu-
Managing Cybersecurity+Risk in Rural Hospitals

TEAHOUSE: Our board is also supportive. My board chair was the first person I called when I found out about our incident. It forced the board to ask a great number of questions. All I could say was, ‘You are correct. Our systems broke down internally.’ We have made significant changes since then. We also share our vulnerability reports with our board, to the audit compliance committee. We meet to discuss the results and assess our risk. Previously, we relied on external systems to back us up, but that didn’t work either. We now have changed our internal systems; they’re a lot harder to crack now.

We’ve also purchased software to protect our phone operating system. For any phone tied to our network, either through email or some other functionality, the software has to reside on that phone. It gives our IT department the ability to kill the phone, wipe it and locate it if compromised. If our employees don’t want that on their phones, then they can use a web browser to access Outlook.

LANDRETH: We don’t allow our employees to use their own devices. In my previous organization, we could bring our own devices. So far, we haven’t met any resistance to our current policy. As to our board, we have a number of new board members. Historically, there has been broad support for IT security initiatives and that remains. They are very engaged and ask tough questions.

STANSBURY: One of the challenges is how to avoid complacency. We have strengthened our systems and policies and educated our staff. It’s similar to all of the alerts that come from our clinical systems. If there are too many, people begin to ignore them. We have a firewall, but I worry that our staff will be too reliant upon the firewall. They feel protected and tend not to worry. I don’t know how to keep people constantly vigilant.
Whenever your third-party vendor releases a patch, it needs to be installed within a couple of days. If not, your organizations are vulnerable to attacks, allowing malware to wreak havoc. With the cloud, you are paying people to do all of this for you. You want to automate as much as you can.

It’s also important to ask your vendors for a vulnerability assessment. It examines everything on your network and looks for vulnerabilities.

**TENHOUSE:** We looked closely at our storage needs and felt we were better off moving things to the cloud, rather than upgrading our hardware and maintaining those systems. Now, our IT staff are able to focus on other things. In the long term, this is a better solution for us. The people in our IT department are flexible enough that they can adapt and learn some of those new responsibilities.

**STANSBURY:** We also did an analysis and it makes sense. Financially, it was awash for us the first five years. We had to go with our guts. We did add staff, as I mentioned earlier. It would have been crazy not to add additional resources. Otherwise, we were only asking for something to happen to us again. Lightning does strike twice.

**AUGSBURGER:** We also felt it was important to add to our staff. We had too for quite some time but, because of new updates, new installs and changing out old equipment, we have greater need. We are changing our EHR system while I’m here at the Rural Health Care Leadership Conference. When we replaced our phone system a year and a half ago, it was my IT staff who actually installed it. We didn’t use a third-party company. As to the cloud, that’s something we need to consider. When it comes to physical backup of our systems, we have a safe room that’s probably 50 to 100 feet from our hospital. If we were to be hit by a tornado, chances are that our backup would be impacted as well. We are working on this.

**BELL:** For those of you who are storing your EHR in the cloud, are you also storing backend systems and your office automation tools there as well? That’s another set of servers that you could eliminate. I recommend two things if you haven’t already done them. The first is backing up everything to the cloud. The second concerns vulnerability management.
MODERATOR: Some of you have mentioned that you participate in local information sharing. Are the rest of you also either locally, or with your state hospital associations, receiving any guidance on this?

TENHOUSE: Education and talking with colleagues are important. The Illinois Hospital Association has been helpful. It has a group of critical access hospitals that meets regularly and cybersecurity is discussed. We have listservs for communication among our peers. If one experiences an attack, we will find out about it quickly. It’s very useful.

AUGSBURGER: I mentioned the Thumb Rural Health Network earlier. And we collaborate with our peers through the Michigan Hospital Association’s Hospital Council of East Central Michigan. We have all kinds of education and data-sharing among ourselves that we can get out quickly.

MODERATOR: What cybersecurity advice do you have for other small and rural organizations?

STANSBURY: It’s reality. It’s no different from investing in fire safety. It’s a necessity.

TENHOUSE: I recommend reviewing IT staffing. Hiring a new person is actually not that big of an operating expense in the grand scheme, compared with the penalties and fines you would pay if there were a major breach.

LANDRETH: We haven’t performed a full financial analysis at this point. How much money would it cost to add an FTE, for example? But I know the board would be supportive of any efforts to protect patient information and protect us from any kind of attack. I do feel we need more support. It’s too much for one person to manage.

TEXT:

Ities. You may find vulnerabilities in older devices and systems that operate off Java or Adobe Flash Player, which are commonly exploited for ransomware.

LANDRETH: We haven’t performed a full financial analysis at this point. How much money would it cost to add an FTE, for example? But I know the board would be supportive of any efforts to protect patient information and protect us from any kind of attack. I do feel we need more support. It’s too much for one person to manage.

MODERATOR: Some of you have mentioned that you participate in local information sharing. Are the rest of you also either locally, or with your state hospital associations, receiving any guidance on this?

TENHOUSE: Education and talking with colleagues are important. The Illinois Hospital Association has been helpful. It has a group of critical access hospitals that meets regularly and cybersecurity is discussed. We have listservs for communication among our peers. If one experiences an attack, we will find out about it quickly. It’s very useful.

AUGSBURGER: I mentioned the Thumb Rural Health Network earlier. And we collaborate with our peers through the Michigan Hospital Association’s Hospital Council of East Central Michigan. We have all kinds of education and data-sharing among ourselves that we can get out quickly.

MODERATOR: What cybersecurity advice do you have for other small and rural organizations?

STANSBURY: It’s reality. It’s no different from investing in fire safety. It’s a necessity.

TENHOUSE: I recommend reviewing IT staffing. Hiring a new person is actually not that big of an operating expense in the grand scheme, compared with the penalties and fines you would pay if there were a major breach.

LANDRETH: We haven’t performed a full financial analysis at this point. How much money would it cost to add an FTE, for example? But I know the board would be supportive of any efforts to protect patient information and protect us from any kind of attack. I do feel we need more support. It’s too much for one person to manage.
It’s important to review the organization’s cybersecurity policies and procedures annually to identify vulnerabilities and to address constantly evolving threats.

Rural health care organizations should look to third-party providers and state and local organizations for support and resources on cybersecurity preparedness.

It’s imperative to avoid complacency among staff by providing consistent communication to keep cybersecurity risks top of mind.

Cybersecurity is more than an IT issue. It requires leadership support, board oversight and constant vigilance across the organization. The American Hospital Association has compiled a resource list to help hospital leaders understand cybersecurity risks, as well as provide actionable tasks to reduce the risk of cybersecurity threats.

**CYBERSECURITY:**
{http://www.aha.org/advocacy-issues/cybersecurity.shtml}
CareTech Solutions  CareTech Solutions is a leader in information technology and end-user interface services for U.S. hospitals and health systems. CareTech’s more than 1,400 U.S.-based professionals create value for clients through customized IT solutions that contribute to improving the patient experience while lowering healthcare costs. From implementing emerging technologies to supporting day-to-day IT operations, CareTech offers clients expert health information technology services. CareTech Solutions is a health IT subsidiary of HTC Global Services, a global provider of IT solutions and business process outsourcing services. Learn more about CareTech Solutions at www.caretech.com.

CareTech’s Data Center Hosting Services have earned the exclusive endorsement of the American Hospital Association.