Operation Cyber-Struck

This fall, RIHCA sponsored "Operation Cyber-Struck" – A series of functional and tabletop cybersecurity exercises. These exercises were designed to test the health center's ability to provide continuity of care and operations during and following a cyber-attack. This gave participating health centers the opportunity to identify areas of strength and areas for improvement and to put systems in place to remedy the areas needing improvement prior to an actual incident. Both exercises were developed by Gail Stout from RIHCA and facilitated by Attorney Linn Freedman from the Law Firm of Robinson & Cole. Each health center was offered both a functional and a subsequent executive tabletop exercise based on the outcome of the functional exercise. There were 8 functional exercises and 7 tabletops conducted.

For the functional exercise, participants were given the following scenario:
At 7:45 this morning, a staff member receives an email and unknowingly clicks on a malicious link. As a result, staff no longer have access to email, phones, remote desktop, VPN, Teams, company intranet, HR software and the Electronic Medical Record.

Next, a patient actor approached the front desk to check in for a sick visit. Participants were expected to demonstrate how the patient would be checked in w/o the use of any IT systems. While all health centers were prepared to transition to paper, it was noted that several health centers only had a minimal number of paper packets printed in advance. In addition, some health centers had no way of knowing who was on the schedules to be seen that day while others routinely print schedules in advance. Participants identified printing schedules a week in advance as a new best practice.

Following check-in, a Medical Assistant brought the patient into the exam room and took vitals and any point of care testing that was indicated by the patient's symptoms. The process for documenting vitals was reviewed.

Next, the provider came into the room to conduct the examination. Participating providers were questioned on how they would verify what medications the patient was currently on, how they would manage patients who needed follow up or referrals and what they would do with the paperwork following the patient visit. At least one health center indicated they no longer had paper prescription pads. There was discussion about how to manage patients who needed controlled substances, which cannot be called in via phone. When questioned about coding and billing, one health center indicated they had a coding sheet included in the paper packets. This was identified as a best practice and shared with the other participating health centers as a recommendation.

The patient then went through the check-out process. All participants indicated the volume of paperwork and organization of all of the packets would be burdensome. One health center utilizes a spreadsheet that is readily available at the front desk in the event of an actual cyber incident. This spreadsheet helps track patients who need to be called back in for re-check, those who may have outside test results or results of any referrals to specialists etc.

On a separate day, an executive tabletop was conducted for leadership to discuss their involvement in dealing w/ the cyber-attack. This piece was tailored to each health center based upon results of the functional exercise. The following topics were discussed:

-Some health centers do not have a Cyber Incident Response Plan (CIRP). RIHCA has begun to plan a workshop that would help with the development or revision of a CIRP.

-Some do not have a dedicated Incident Response Team (IRT). Participants were advised to use the senior leadership team meetings and dedicate time in the agenda to discuss development and implementation of best practices identified during both exercises.
-Participants were encouraged to ensure members of the IRT had personal cell phone numbers of all members in their own cell phone.
-Communication with staff, patients and media. Scripted communications were advised.
-Communication with the answering service. Can they manage a surge? What they tell patients.
-CAP agencies discussed process for notifying programs outside of the health center and how to manage their services.
-Process for billing.
-The process of filing a claim with the cyber insurance carrier and working with the appointed attorney and communications with the threat actor.
-Demand for ransom and each health center's approach (to pay or not to pay).
-IT staff roles during the incident.
-Process for standing up backup servers.
-Use of personal devices to access systems remotely.
-Prioritization of business-critical systems.

A special thank you to RIHCA staff actors and our community partners from HCRI and RIDOH.
-Elena Nicolella, RIHCA
-Hannah Marston, RIHCA
-Shelley Sousa, RIHCA
-Dawn Lewis, Healthcare Coalition of RI
-David Balbi, RIDOH
-Rupsha Biswas, RIDOH
-Ratha Sen, RIDOH