BECKER'S
HOSPITAL REVIEW

24 healthcare leaders reveal how they're always evaluating cybersecurity

Randi Haseman – July 24, 2023

Three healthcare data breaches affected over one million people. More could be impacted in the future since their third-party vendors may use the file-transfer application from Progress Software.

At the same time, HHS and FTC are warning hospitals and telehealth providers about cybersecurity risks posed by online tracking technologies integrated into apps or websites.

These 24 industry leaders share how they are continuously assessing current cybersecurity measures at their systems. The executives featured in this article are all speaking at the Becker's Health IT, Digital Health + RCM Annual Meeting: The Future of Business and Clinical Technologies which will take place Oct. 3-6, 2023, at the Navy Pier in Chicago.

As part of an ongoing series, *Becker's* is talking to healthcare leaders who will speak at our conference. The following are answers from our speakers at the event.

Question: As the cybersecurity landscape continues to get more intense, how do you plan on prioritizing the assessment of your current cybersecurity measures?

Mike Mistretta, Senior Vice President and CIO at VHC Health (Arlington): Cybersecurity will always be in the forefront of everything we do in the IT space in the health system. As bad actors get more sophisticated and attacks more intense, health systems will be forced to adjust or pay the penalty by becoming victims. Prioritizing security initiatives will be a matter of risk assessment and tolerance — the higher the risk and lower tolerance, the higher we will prioritize the project.

Laura Smith. CIO at UnityPoint Health (West Des Moines, Iowa): Cybersecurity must become a top priority in health care as the industry continues to be a prime target. I believe this starts with ensuring the risk tolerance and framework of your cybersecurity program is approved by your governance board. Having this framework in place at UnityPoint Health allows our teams to constantly assess and more quickly re-prioritize risk mitigation plans as necessary.

Michelle Stansbury. Vice president of innovation and IT applications at Houston Methodist: Healthcare systems are increasing their digital footprint to satisfy the demand of our customers, and it has become increasingly important to take appropriate cybersecurity measures to protect institutions from external threats. Cybersecurity has always been a top priority for Houston Methodist, and we have implemented several best practices to ensure we're protecting ourselves from external threats. Some of those include: regularly conducting security audits and penetration testing to identify weaknesses and potential entry points for attackers; incorporating strong access controls to limit access to sensitive information or critical systems; and conducting third party risk assessments to identify potential vulnerabilities.

Now, more than ever, we have become accustomed to utilizing technology in our daily lives whether at work or home, and we will continue to prioritize cybersecurity measures as the landscape evolves.

Steven Ramirez. Chief information security officer at Renown Health (Reno, Nev.): We have a big emphasis on security assurance. We won't know our deficiencies if we don't have a framework (MITRE and NIST CSF) to measure our maturity/capabilities against. We reprioritize our measures based on those findings.

My primary focus has always been on early detection, vulnerability management and access management. If we do those right, we can have the baseline to mitigate a majority of changing risks. I like to take an approach similar to risk and emergency management with an all hazards approach. This is a preparedness lifecycle that enables us to build out a framework to adapt to various types of risk. This helps drive our adaptive defense in depth model. It is also a model that my healthcare leaders and peers at my organization can relate too.

Onyeka Nchege. Senior vice president and CIO at Novant Health (Winston-Salem, N.C.): Novant Health employs a cybersecurity program that addresses electronic information and information systems that support business processes and assets of Novant Health, including those provided or managed by another organization, vendor or source. We collaborate across departments on this program, including a comprehensive framework of cybersecurity activities, outcomes and controls that provide detailed instruction for developing, implementing and maintaining cybersecurity.

Jason Szczuka. Chief digital officer at Bon Secours Mercy Health (Cincinnati): BSMH continues to refine a data-driven approach to prioritizing our assessments of our cybersecurity program. We collect, analyze and aggregate internal data from cyber-risk assessments. We incorporate input from internal and external audit teams. Just as important is actual event and incident data. We take a page from peers in patient safety by focusing upon lessons learned from NMEs or 'near-miss events.' For external data drivers, we rely upon diverse government sources: DHS, CISA, FBI, FDA, NIST, HHS, OCR. Private sources include ISAC, HIMSS, CHIME and OWASP. Because we have international operations, we must also embrace the complexity of international frameworks from the EU and ISO.

Rick Jiggens. Principal cybersecurity engineer at Kinwell Physician Network (Seattle): I prioritize my current cybersecurity measures by first conducting a comprehensive risk assessment to identify areas of vulnerability. Next, I protect my most critical assets, such as PHI, by enhancing their security measures. I regularly review the effectiveness of these measures through security testing, penetration testing and of course phishing simulations. All the while, I ensure we are following relevant regulatory requirements. These measures are done in a continuous cycle to stay up to date and to consider new and emerging threats.

Ash Goel, MD. Senior vice president and CIO at Bronson Healthcare Group (Kalamazoo, Mich.): We believe that the speed of evolution of the landscape requires a methodical approach to evaluating trends and creating mid to long-range plans. The team has long used the National Institute of Standards and Technology Cybersecurity Framework to understand and organize the approach. We create annualized plans which target long-term improvement, resiliency and usability, allowing us to be wise in our investments in newer tech.

Of course, all of this also requires us to stay on top of the emerging threats. We have built a strong network of relationships with peers, industry experts, insurance experts as well as technologists to constantly gather input, adjust the ongoing plans and evaluate opportunities. Cybersecurity practices clearly can't stay on an island, even though we keep building walls around organizations, knowing that threat actors are always probing our defenses for weaknesses.

Zafar Chaudry, MD, MS, MIS, MBA, CITP. Senior vice president, chief digital officer and CIO at Seattle Children's: At Seattle Children's, we continue to prioritize our readiness against cyber threats. We do this by continuous identification and assessment of our assets; performing annual risk assessments with key stakeholder input to identify potential vulnerabilities and threats that could exploit our assets; evaluating our existing cybersecurity controls, policies and procedures to determine their effectiveness in mitigating the identified risks; and assessing if they align with industry best practices and compliance requirements. We prioritize the vulnerabilities and weaknesses that pose the greatest risk and implement the necessary security controls. We also continuously monitor and test our cybersecurity measures to ensure their effectiveness. In addition, we develop robust incident response plans that outline the steps to be taken in the event of a cybersecurity incident while we stay informed about emerging threats and vulnerabilities in the cybersecurity landscape.

Phil Alexander. Chief information security officer at North Mississippi Health Services (Tupelo, Miss.): The prioritization of cybersecurity measures begin by looking at and evaluating: direction of organizational priorities over the next one to two years (i.e. cloud, mobile apps, remote work, etc.); the current and projected threat landscape; and Cyber Security Frameworks (NIST/CSF, HITRUST and ISO).

Shenny Sheth. Deputy chief information security officer at Centura Health (Centennial, Colo.): Centura has made an attitudinal start by identifying the most critical assets we have in our possession. This could be sensitive data, customer information or mission-related infrastructure resources. Our teams quarterly evaluate implementation and effectiveness status of the existing cybersecurity controls and measures/safeguards to tune-up critical assets via a formal cyber program. We rely upon robust system acquisition steps with insights from a continuous threat and vulnerability management program to identify

potential attack surfaces. We recently made foundational policy changes, developed modern security standards and adopted architecture patterns to promote guardrails, process guidance and special diligence requirements for patient-facing operations — all while considering the possibility of a successful cyberattack. We remain tactical with critical assets and stay situationally informed about the current threat landscape to ensure cyber adversarial activities do not realize harm to our enterprise.

Prasanna Menta. CIO at Sheppard Pratt (Baltimore): To effectively evaluate the state of cybersecurity measures in an increasingly challenging landscape, organizations need to adopt a risk-based approach. This involves several key steps: identifying critical assets, conducting regular vulnerability assessments and staying up to date with emerging threats. It is also important to invest in fostering a culture of security within the organization and among its consumers, establish an effective incident response plan and ensure compliance with relevant regulations. Implementing continuous monitoring and patch management processes, as well as conducting regular reviews and updates, are crucial for adapting to evolving threats.

By following these steps, organizations can establish a robust cybersecurity program that not only assesses the current environment but also demonstrates their commitment to security now and in the future. Furthermore, such a program offers additional benefits, including cost reduction in areas like skyrocketing cybersecurity insurance, building trust with consumers and partners, and reducing the risk of financial loss.

Ty Faulkner. Professor of health information technology management at Lawrence Technological University (Southfield, Mich.): To improve cybersecurity measures, assess your organization's compliance with the HIPAA Security Rule requirements starting with risk analysis and risk management of network servers, the largest category for healthcare breaches. Also, assess your organization's information system activity review and review your audit controls and access controls. Finally, increases in budget allocation may be warranted for higher levels of access controls to strengthen your organization's authentication processes to help impede or prevent many cyberattacks.

Jordan Moskoff, MD. Medical director for adult emergency services department of emergency medicine at Cook County Hospital (Chicago):

Given the enormous downside of a potential cybersecurity breach, we prioritize ongoing risk assessment to consistently examine the global picture and determine where to best focus our effort.

We monitor our most valuable and sensitive assets, such as patient data, financial records and infrastructure, and prioritize these areas for a risk assessment. This assessment evaluates potential risks and vulnerabilities that could impact operations and allows us to prioritize vulnerabilities based on severity, likelihood of exploitation and potential impact.

After analysis, we then implement additional or strengthened security controls such as firewalls, intrusion detection systems, encryption, access controls and security monitoring tools. Similar to our work monitoring critically ill patients in the ED, we must actively reassess the cybersecurity landscape. To this end, we regularly review and update our security strategy, stay informed about emerging threats and new technologies and adapt our cybersecurity measures accordingly.

Brian Shea. Interim CIO at Lexington Clinic (Ky.) and CIO at MedOne Healthcare Partners (Columbus, Ohio): As it is widely acknowledged, the cybersecurity arena undergoes constant evolution. One constant, however, is cybercriminals' persistent exploitation of novel technology and social engineering methods to target organizations and individuals, seeking financial gains or causing disruptions. It is crucial for organizations to remain vigilant and integrate security into their very core, becoming an inherent aspect of both the organizational and individual mindset. In essence it must be a part of the organization's and/or individual's DNA. To effectively tackle the ongoing cybersecurity challenges, organizations must consistently adapt their approaches from the perspectives of people, process and technology. So, prioritization of assessment of the cybersecurity measures should also be a continual on-going effort.

John Finkbeiner. Senior clinical informaticist at South Shore Hospital (South Weymouth, Mass.): This is something we have worked on extensively and continue to do so. We began by revamping our network infrastructure to add extra layers of security. In order to further secure the network, however, we are moving towards all employees having a single sign-on. This will involve multi-factor authentication, a complex password no less than 12 characters and a physical USB 'key' to log into the system.

Jonathan Westall, FACHE. Vice president of ancillary services at Martin Luther King, Jr. Community Healthcare (Los Angeles): We have moved forward with a mandatory steering committee that encompasses all classifications of employees, especially as we see more and more broad-based attacks that hit every email. What might be common sense to a cybersecurity practitioner is a foreign language to some of line staff skilled in other areas. These steering committee meetings ensure we focus on a comprehensive program that ensures cybersecurity is practiced by all individuals within our organization.

Joel Klein, MD. Senior vice president and CIO at University of Maryland Medical System (Baltimore): Even if it starts raining harder when you have to go out, you still start with an umbrella and good rainwear. We're thinking about our cybersecurity investments in the same way as the volume of cyberattack activity in the healthcare industry goes up and down. It starts with a thorough, candid and externally validated risk assessment that is then matched to our controls. You then map that to where you stand today, taking into account an equally honest conversation about risk tolerance, and map out a multi-year plan.

From there, there's two other things we've found critical. One is balancing the temptation to play whack-a-mole and take your eyes off this bigger picture against stopping to address truly critical problems as they come up. The second is remembering that cybersecurity is not the only imperative we have in a large, complex healthcare delivery system, and we have to balance our investments, attention and bandwidth against all risks and opportunities, not just one flavor.

Fred Cushner, MD. Lead orthopedic surgeon at Hospital for Special Surgery (New York City): Canary Medical performs regular assessments of its security and privacy profiles to ensure compliance with the ever evolving cybersecurity laws and guidelines. We currently structure our operational practices and infrastructure in accordance with NIST standards, SOC2, and HIPAA and HiTECH laws.

Jahmela Pech, DNP, RN. Executive director of quality management at Providence St. Joseph Hospital of Orange (Calif.): Providence St. Joseph Hospital Orange understands the increasing threats in the current cybersecurity landscape. Our cybersecurity program is aligned with the set of guidelines by NIST CSF. It establishes the standards in assessing our current cybersecurity

measures. We engage independent third parties to assess our cybersecurity maturity on an annual basis. We have a variety of cybersecurity vendors and partners supporting us with people, processes and technologies to maintain our program. Intense collaboration between departments, leaders and staff is critical in protecting the confidentiality, integrity and availability of information.

Lisa Ivanjack, MD, MHCM. CMO for PeaceHealth Medical Group at Columbia Network (Vancouver, Wash.): A key area that we focused on in our assessment of cybersecurity measures recently was that of continuity of the ability to provide clinical care to our patients. My health system had already done some work on the inpatient side and expanded that work recently to include the outpatient departments. Devoting time, attention and resources to proactively develop a robust plan for providing clinical care to patients in the event of a prolonged downtime is vital work.

Bradley Locke, DO. Chief medical information officer at Prevea Health (Green Bay, Wis.): Change has dominated the landscape of cybersecurity over the last 15 years, but what has stayed consistent is the overall risk assessment process. It is imperative to systematically approach risks and threats, catalog potential risks, expand areas of assessment, and add innovative technologies and resources; however, throughout it all, the risk assessment process itself remains the same.

Raymond Lowe. Senior vice president and CIO at AltaMed (Los Angeles): Cybersecurity is always at the forefront of our services and work. A robust cybersecurity program will ensure that appropriate safeguards are properly selected, implemented and monitored in every aspect of how we function as an organization. Frameworks, like NIST 800-30, NIST CSF, HITRUST CSF, ISO27001 and others safeguard that we are able to provide a comprehensive and consistent structure to help an organization work towards regulatory compliance. At AltaMed Health Services, we are aligning our cybersecurity program to NIST 800-30 based on risk and threat assessment processes to identify potential threats that could significantly increase risk. Next, we measure the strength of our existing controls against the NIST Cybersecurity Framework to identify potential control gaps as well as opportunities for improvement. We then use this information to recognize control initiatives, addressing the highest risk items and prioritizing efforts that both reduce business risk and improve our overall control strength. As the cyberthreat landscape continues to evolve and

shift, our team and partners work collaboratively to access and pivot to address these ongoing challenges.

Steve Davis, MD. President and CEO at Cincinnati Children's: For our organization, our leadership and compliance teams have identified cybersecurity as a tier one risk, and so it is paramount that we continue to evolve and adapt our cybersecurity policies and strategies to address the ever changing cyber landscape and growing risk. We first must continue to ground ourselves against the security frameworks (CIS, NIST, HITRUST) that our organization uses to guide and measure our security policies and initiatives. From there we will continue to use third parties to help assess our controls and see where our gaps and improvement opportunities exist. From these external assessment and framework reviews, we will need to continue to prioritize these projects, but also ensure that we are delivering the technologies and capabilities for our organization to deliver care for our patients. Lastly with ransomware still being a threat that could impact our organization, we must ensure that we continue to have the security tools and processes in place that can respond to this type of event without a significant impact to patient care — continuation of network segmentation initiatives, table top exercises, endpoint security, and securing backup and recovery to critical systems.