EXECUTIVE INSIGHTS

RESILIENCY + RECOVERY

THIRD-PARTY RISK AND DATA SECURITY FOR HEALTH CARE IN A CLOUD NATIVE WORLD

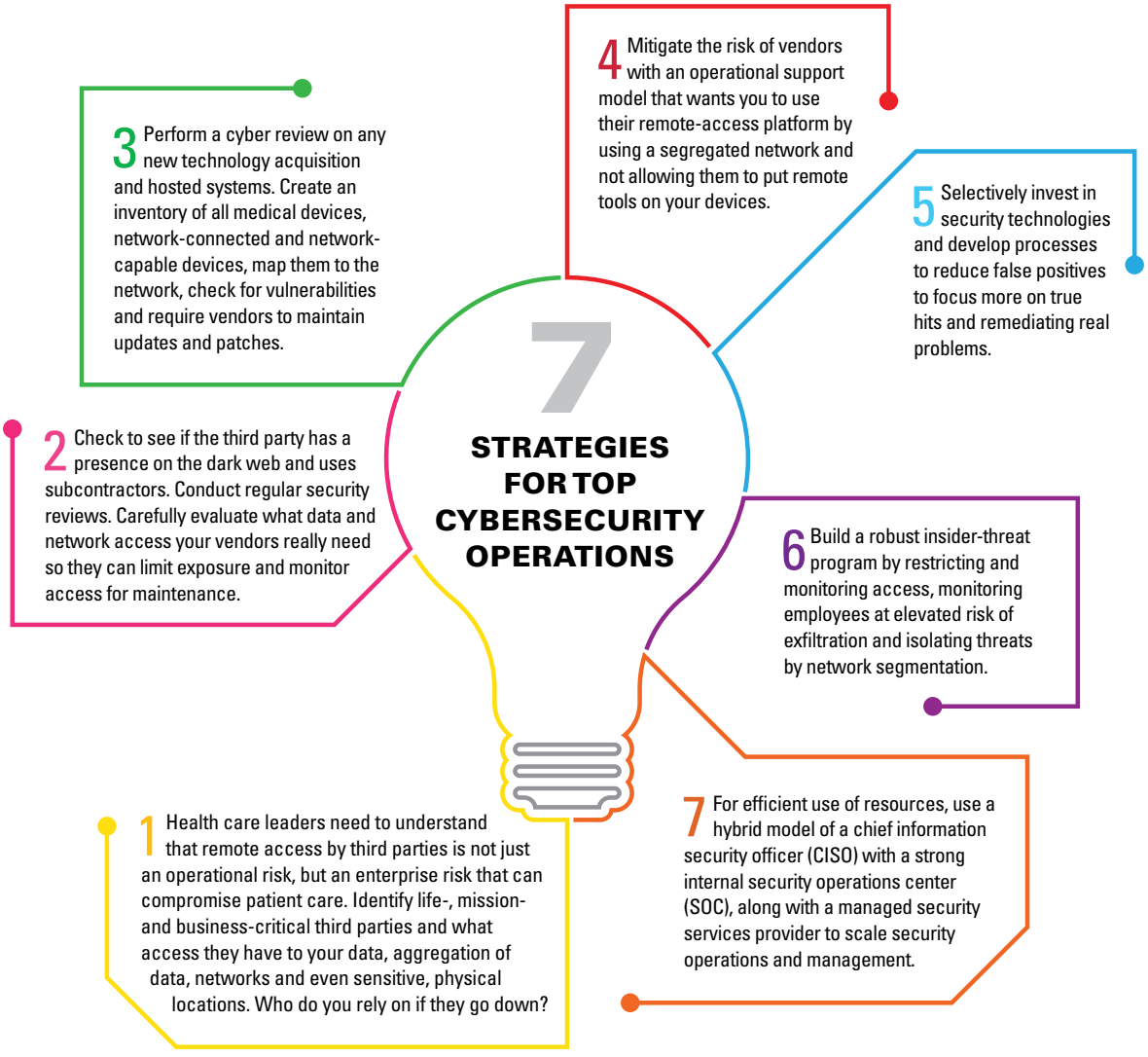
Maximizing the value of security operations and technology investments

SPONSORED BY: American Hospital Association™ | BlueVoyant

Third-Party Risk and Data Security for Health Care in a Cloud Native World

Maximizing the value of security operations and technology investments

The move to the cloud and the use of electronic health records has multiplied the number of third parties with access to a hospital's sensitive data, increasing the attack surface. When hospitals and health systems do business with a third party, security becomes a shared responsibility. Inadequate security policies and controls within a third-party provider can lead to a compromise of the organization's network, data or services. This executive dialogue examines how hospitals and health systems are introducing internal and external threat detection and response to defend data from internal, external and third-party threats in a cost-effective manner.



PARTICIPANTS

Ryan Allen, MSHA, CISSP
ASSISTANT VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER
UAB HEALTH SYSTEM | BIRMINGHAM, ALA.

Adam Briggs, J.D.
CHIEF COMPLIANCE OFFICER
MAYO CLINIC | ROCHESTER, MINN.

Bruce McDaniels, MBA, CISM
VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER
PARKLAND HEALTH | DALLAS

Michael Minear, MS, CHCIO, CPHIMS
SENIOR VICE PRESIDENT AND CHIEF INFORMATION OFFICER
LEHIGH VALLEY HEALTH NETWORK | ALLENTOWN, PA.

Milan Patel
GLOBAL HEAD OF MANAGED SECURITY SERVICES
BLUEVOYANT | NEW YORK CITY

Mark Rubinoff, Esq.
VICE PRESIDENT, SPECIAL COUNSEL FOR TECHNOLOGY AND INTELLECTUAL PROPERTY
THOMAS JEFFERSON UNIVERSITY AND HOSPITAL | PHILADELPHIA

Kelly Walenda, Esq.
ENTERPRISE CHIEF PRIVACY OFFICER
THOMAS JEFFERSON UNIVERSITY AND JEFFERSON HEALTH | PHILADELPHIA

MODERATOR **John Riggi**
NATIONAL ADVISER FOR CYBERSECURITY AND RISK
AMERICAN HOSPITAL ASSOCIATION | WASHINGTON D.C.

MODERATOR JOHN RIGGI: *(American Hospital Association):* **The move to the cloud and the use of electronic health records (EHRs) has multiplied the number of third parties with access to hospital-sensitive data. We've expanded our attack surface dramatically, especially during the pandemic where we had a rapid deployment of remote connected technology, not only for our workers, but also increased reliance on a third-party cloud base, third-party providers. Foreign-based cyber criminal organizations and hostile nation states did not give us a humanitarian pause during the pandemic. They increased cyberattacks against us, and the situation in Russia and Ukraine is only increasing the cyberthreat. Hospitals could become collateral damage in either a ransomware or destructive malware attack aimed at U.S. critical infrastructure, financial services or the energy sector. One of our cloud-based, mission-critical, life-critical or business-critical third-party providers could become victim of a destructive or disruptive cyberattack.**

What is your hospital or health system doing to ensure that third-party vendors and service providers take the proper steps to protect sensitive information? Let's start with Milan Patel, head of BlueVoyant's global managed security services and a former FBI agent like me, by asking, 'What steps are organizations taking?'

MILAN PATEL *(BlueVoyant):* A couple months ago, we identified a third-party supply chain risk involving a large health care system that we provide with managed services and deep and dark web threat intelligence services. We learned that somebody was logging into an application within their purview as a customer success manager for this third-party, siphoning out financial and patient data from the platform and then taking those data and putting them for sale on the dark web.

We were combing the dark net, looking for telltale signs of any activities that could be connected to any one of our customers — what we call chatter. We were fortunate enough to find and interact with this individual to figure out what kind of data they had, and they gave us a data sample. We went back to our customer and asked, 'We've got some data that we think is yours. Based on the material, can you tell us where it could have come from?'

They identified three separate applications where the data existed; one was internal and two were external. One was a third party managing an application that had access to the same data. We immediately began conducting a proactive threat hunt across their entire environment of 50,000 devices, globally looking for somebody trading data externally, and trying to help the health system identify where the leak could have happened if it wasn't internal.

They identified the vendor that was hosting the data on their behalf. This particular vendor had access to more than 4,000 other hospitals, providing similar financial services. We notified the vendor and got in touch with their CISO. It turns out that an employee was logging into these databases from home and siphoning off data via a VPN.

While we were conducting this forensic investigation, we found that the employee had access to 40 other hospitals. I immediately notified John of what we had found to make sure we were ready to notify those hospitals. If there is a problem, it's the right thing to do, whether they're our customers or not.

This example highlights a couple of key issues. When we talk about vendor risk management, we typically talk about a questionnaire that you expect an organization to fill out that confirms it has firewalls and has performed a pen test. You might ask for copies of the pen test, a past management schedule, the mean time to patch and vulnerabilities high through low.

Our health care system customer pulled out the

questionnaire of this particular vendor and all the check boxes were filled out. However, they didn't have great control over who accesses their applications at what times and what days.

First, after that initial point assessment, what else should an organization be doing — either proactively or through some monitoring to make sure that this third-party is patching vulnerabilities on their public facing infrastructure? Second, how do you then hold them accountable after identifying things that are problematic? In larger organizations, we find that there's a relatively small group of people, maybe 10, managing thousands of vendors and suppliers that are connected to the hospital system. We're talking about the organizations that are allowing access into their environment to view data from a third party or shipping data to a third party. Those relationships are a separate facet that third-party risk is not really designed to handle.

We typically see that problem falling on the CISO. In the past, the CISO would refer us to the procurement team when we wanted to talk to vendors. Now the CISOs are telling me, 'I'm worried about this vendor because if I get breached, it's going to come from them.'

RYAN ALLEN *(UAB Health System):* We're taking several steps to mitigate third-party risk that have been helpful. As part of every contract review, especially those that have access to PHI or if we share sensitive information with a third party, we do a security review.

We use SecurityScorecard and then we do quarterly reviews, just rescans of all the vendors with whom we share that information and look for drops in their score. If they were a 90, which is not too bad, and they drop to a 75, we'll follow up with them to see if they're more vulnerable than they led on with their initial application.

We also stopped giving vendors everything they asked for and started evaluating what they really needed. Companies would send us a spreadsheet of all the data fields they wanted in the interface or the systems to which they thought they needed access. We stopped accepting those requests and started asking exactly what it was they were going to be doing, and then we work with them to determine what data they really need.

"Companies would send us a spreadsheet of all the data fields they wanted in the interface or the systems to which they thought they needed access. We stopped accepting those requests and started asking exactly what it was they were going to be doing, and then we work with them to determine what data they really need."

— Ryan Allen —
UAB Health

That limited our exposure. Few vendors need Social Security numbers (SSNs), yet just about everyone asks for them. We also have good contract language about notification. Anytime there's an issue on their end, whether they know it's a breach of our data, we require notification within 24 hours so that we can double-check on our end.

We control the user accounts that come back to us. Anybody who's connecting back into the system goes through active-directory accounts that use our multifactor authentication.

If they're going to access a system for maintenance, it must be during business hours unless otherwise approved. If somebody needs access back into our system, 95% of the time we make them use our remote access tool. An employee of the health system must accept that connection so that they can do their work.

We also use Recorded Future for our threat intelligence. We look at vendors in the contract review and sometimes on an ongoing basis, depending on how much information we're sending them.

MODERATOR: I want to emphasize a couple of points Ryan made: He checks to see if the third parties they have contracted with are appearing in chatter on the dark web. Is their data appearing on the dark web?

The other thing you mentioned is that often organizations fail on a strategic level to identify their life-critical, mission-critical and business-critical third parties — the vendors you depend on for those services. Who has your data; who has an aggregation of your data; who has access to your networks or even sensitive, physical locations? Who do you rely upon as a backup if you lose their services due to a cyberattack and what are your business continuity plan and downtime procedures if they go down?

For example, hospitals did not realize how Kronos folks hadn't thought about how mission-critical and business-critical Kronos was to their operations. Another company, Elekta, provides the software that runs linear accelerators that deliver radiation therapy to cancer patients. They were hit with a ransomware attack last year, which resulted in radiation oncology being disrupted at 42 major health systems across the country and ultimately delaying cancer treatment for patients for up to three weeks.

BRUCE McDANIELS *(Parkland Health):* We're doing similar things to tighten up our third-party risk. One of the biggest challenges we have is arm wrestling with vendors that are either sole-source or the market leader. We rely on their services, but their operational support model is 'We're not going to use your remote-access platforms to access what we need to maintain. You're going to use ours.' I'm paid to manage the security for my hospital system and not to facilitate the ease of their support model, which ultimately is the argument they're making. I'm curious if you've had similar struggles and what you've done to mitigate those risks.

ALLEN: In our organization, I'll take it to the senior vice president of the area that works with the vendor and explain the risks and our policy and ask them, 'Do you want to assume the responsibility for this company having its own type of remote access, because I said no?' I let them know that they can overrule me by going to the CEO or my chief information officer (CIO), but it's going to be documented. Generally, they'll have a conversation with the vendor who will say, 'Well, what can we work out?'

"Often organizations fail on a strategic level to identify their life-critical, mission-critical and business-critical third parties — the vendors you depend on for those services. Who has your data; who has an aggregation of your data; who has access to your networks or even sensitive, physical locations? Who do you rely upon as a back up if you lose their services due to a cyberattack?"

— John Riggi—
AHA

We found a good compromise. Let's say that they use virtual network computing (VNC). We use BeyondTrust. I'll let them use VNC into a jump box on our network. That's segregated out in the demilitarized zone, a subnetwork that protects and adds an extra layer of security to an organization's internal network from untrusted traffic, but then they must use our system to get to specific equipment or other devices for support, or even remote desktop protocol once inside the network. They can use their tool to initiate the request, but once inside the network, I have more control of where they're going and what they can access. It's not ideal, but it makes me feel better. I won't let them put their remote tools on our devices.

MODERATOR: That's an excellent strategy. Cyberrisk is enterprise risk, business risk and obviously a risk to patient care and safety. When the business owners must document that they're

willing to assume the risk, it's a risk for the entire enterprise, not just for their business operation. If that vulnerability was used to deliver ransomware into the organization and interrupt patient care, they unilaterally accepted risk on behalf of the entire organization.

ALLEN: I'm assuming your vendors, when they're pushing back, are saying that we even wrote it into the contract that this is what we use. The business owners are trusting the lawyers that they're going to not only know the law, but also all internal policies. And it doesn't work out that way.

McDANIELS: In our case, most of our leaders, especially our clinical leaders, are just looking for the capability. Those details are not top of mind for them. I like your idea with the jump box. If I could strike a compromise that allows them to use their tools to a certain extent, and then demark into our organization using our tools, I think that would be a better solution. I need to see how that would work.

MICHAEL MINEAR *(Lehigh Valley Health Network):* We have a small team and hundreds of systems to manage. We've been successful in preventing any new technology from being acquired and put into use for which we haven't done a cyber review. We have a team comprising technology, legal, and our privacy officer involved when we negotiate vendor contracts.

Unfortunately, we have a queue of about 30 new technologies on which we're trying to do a cyber assessment at this time. We struggle to do a re-review sometime after the initial cyber assessment to ensure everything is current. We have different tools that we can use for hosted systems versus trying to do a full review of a vendor that we host locally.

"One of the biggest challenges we have is arm wrestling with vendors that are either sole-source or the market leader. We rely on their services, but their operational support model is 'We're not going to use your remote-access platforms to access what we need to maintain. You're going to use ours.'"

— Bruce McDaniels—
Parkland Health

In sharing sensitive data with outside consultants or vendors, we find that some of the vendors or consultants use subcontractors, and some may hide that relationship. We must make sure we know what any subcontractor is doing, whether they are offshore, and how they are securing our organization's data. It's a struggle to staff the cybersecurity reviews. We are using many of the hosted technologies that John talked about initially and I don't see that slowing down.

PATEL: The organizations we help are medium-sized to enterprise; they're not going to get the resources to build their own SOC. They're outsourcing as best they can. We've found the hybrid model is successful with the CISO having an internal team of two or three strong people and outsourcing SOC-as-a-Service. But the reality is that you can't afford to only outsource SOC-as-a-Service and do nothing else and expect that your SOC remote is going to take care of all your problems. SOC-as-a-Service is designed to scale and do the heavy grunt work of security operations and security management. For the day-to-day, higher-level touch with end users, you need managers inside the organization — an internal team qualified to handle digital forensics and response, network and traffic capabilities and the security products. SOC remote will do the heavy lifting and notify you when there's an escalation and we need your help to interact with either end-user support or something else.

For example, we're providing services for a large organization, roughly 50,000 endpoints and 44,000 hospital professionals. Last year, we processed 750,000 alerts for this hospital. We escalated 3,000 and found a few true confirmed positives. That requires time and commitment to do at scale. I tell

customers that if you're going to move to the cloud, your only option is to look for outsourcers that are already in the cloud using similar technologies, whether in Microsoft, Amazon Web Services (AWS) or Google Cloud Platform. You will all be in the cloud at some point in the future via a third party, or all your existing applications of workloads will be in the cloud. There's nothing left on premise besides some dummy terminals. That's just the reality we live in.

MODERATOR: This massive movement to the cloud without on-premise backup solutions and capabilities for life-critical, mission-critical, business-critical systems concerns me. Leaders have to understand the risk they're creating when they move to the cloud. Since malicious insiders use valid credentials, what is your information technology department doing on the inside to stop it? While we're focused on external threats, we still have the internal threats and potentially hybrid threats where internal individuals are working with external hackers.

ADAM BRIGGS *(Mayo Clinic):* We've matured our non-employee access program and our insider-threat program to increase monitoring of employees we consider to be more high risk or elevated risk of exfiltration. We're also pursuing segmentation of systems. So that access to one piece of the network doesn't necessarily grant an employee access to all.

As of 12 days ago, we fully removed patient SSNs from the demographic field in our Epic system. That is one less vulnerability than we had a few weeks ago.

MODERATOR: That's fantastic. If you don't need it, why is it there? It just presents vulnerability and risk in so many ways. Milan, regarding insider threats, how do you handle those or help hospitals and health systems?

PATEL: The problem is that there are many vendors with overlapping capabilities. One gets tired dealing with Netskope (a secure access service edge cybersecurity concept), the Microsoft version of Netskope and other versions. What are the right controls to drive the behaviors that you want in your organization without slowing down the business? The challenge is that integrating these tools in a single place that drives some sort of outcome has become almost impossible. What ends up happening is that you have 30 tools and they're all great. The vendors have told you they're awesome. And now you're trying to figure out what the correlation is going to look like between Netskope and a firewall or a firewall and some other identity solution.

"The organizations we help are medium-sized to enterprise; they're not going to get the resources to build their own SOC. They're outsourcing as best they can. We've found the hybrid model is successful with the CISO having an internal team of two or three strong people and outsourcing SOC-as-a-Service."

— Milan Patel—
BlueVoyant

I tell a lot of CISOs who have this technology sprawl to figure out what the use cases are they want to solve for, prioritize them, figure out what tools are going to do that work, and then create a plan to do that.

MODERATOR: Often when CEOs understand that cyberthreats equate to massive operational risk, they start to throw money at cybersecurity technology. However, the funds may be wasted if correlating cybersecurity spend with impact on risk reduction, especially risk reduction to care delivery and patient safety. You may be wasting your money if you're not correlating for best impact. Often our cybersecurity professionals spend more time chasing false positives than dealing with actual security incidents. Unfortunately, this is a common complaint.

McDANIELS: Following up on what Milan said, when I moved into my role, I inherited a sea of technology. I started looking at all the platforms we had and realized that there was a lot of capability, but not much was turned on. I had security professionals that were functioning as systems engineers and platform owners. They weren't performing their security functions. Over the last several years, I've spent a lot of time doing platform rationalizations and trying to squeeze it down to a subset of basic world-class capabilities that my limited team can be expert in.

Another approach that I'm taking is trying to push as many of the capabilities that I have in house to a service model. I'm letting vendors manage the platforms. My small security team can then truly be security experts and protect our environment.

MODERATOR: With the increasing proliferation of the internet of things and internet-enabled health care devices, what's your cybersecurity team doing to keep track of and have visibility into the data across all those devices? One of the biggest gaps I've seen across the country is that network-connected and internet-connected medical devices are under the control of clinical engineering, not the CIO. That gap creates vulnerability when it comes to patching, network mapping and basic inventory.

MINEAR: I couldn't agree more that the big threat is the internet of things and medical devices. We integrated clinical devices, or clinical engineering as we call it, with our technology division about three years ago. The first thing we did was an enterprisewide physical inventory of our devices. It had never been done before. We also have linked physical clinical devices with their network address and usage, and we have fully segmented all clinical devices on our network. We have newer tools that show sophisticated technical and network usage profiles for clinical devices and classes of devices, which provides a critical level of detail and alerts not available only a few years ago.

We don't add a new clinical device to our network without doing the cyber review. We always work in partnership with our clinical leaders. That partnership has facilitated a more sophisticated knowledge base around clinical devices and made our response more effective.

Lastly, we have to challenge the clinical device vendors around cybersecurity. The FDA is starting to challenge the vendors, which is great. If you do an inventory and track how long you've used a lot of the clinical devices, many have been in use 10-15 or more years ago and created in a time when cybersecurity was not understood or was a priority. The fact is some clinical device vendors don't have a technical platform that they can secure, and most will admit that once we call them on it. When vendors have a new model coming out, they must make sure they fix the cyberrisks in their new generation, as their customers will use these devices for many years into the future. As clinical organizations, we should hold clinical device vendors accountable and make sure they secure their products.

MODERATOR: Because medical devices are the technology that is closest to the patient, cyberrisk in those devices pose the most immediate risk to patient safety. The CEOs and the regulators understand that.

The FDA has a slick sheet out that tells the vendors that they can upgrade their devices for cybersecurity purposes without FDA authorization. Also, I would encourage all to support pending federal legislation known as the PATCH Act, which will impose requirements on medical device manufacturers to increase the cybersecurity of medical devices over the lifespan of the device.

How are data privacy-compliance regulations impacting your ability to work with managed security service providers, or are they?

PATEL: Knowing what data belong in a security ven-

dor's portfolio of access is important through a Security Information & Event Management (SIEM) or an Endpoint Detection & Response (EDR) solution. Sometimes it gets challenging. We integrate Epic into SIEMs and the customers want specific detections on the misuse of Epic, and those are powerful capabilities.

Our job as a vendor is to make sure that those detections don't yield anything that could be private to the hospital. There are security metadata, not necessarily raw access to any of the login data for the patient or health care provider.

In the last three years of organizations' moving to cloud native SIEM and EDR technologies, there's a cultural change in how CISOs think about where their security data are going. They prefer that the data reside in a platform or a warehouse that they own in their tenant — AWS, Microsoft Azure, pick your service provider — which can be locked and access given to it when needed. We're seeing CISOs gravitate toward that model and completely changing the way they think about where their security data are being hosted and correlated.

MODERATOR: That's an interesting trend. As we move to the cloud, I'm always concerned about what happens when we lose the internet connection to the cloud provider. Whether you are attacked and you must disconnect from the internet to prevent the ransomware from spreading or for whatever reason the internet connection is lost, what will be the impact to health care delivery in your organization? How has your organization changed its security protocols in relation to the elevated cyberthreat posed by the Russian invasion of Ukraine?

MARK RUBINOFF *(Thomas Jefferson University and Hospital):* One of the things we did at Jefferson Health was send out fake phishing emails, put out blast emails to see who would click on the phishing attempt and who would click on the item that reports the phishing to educate people and to get a better sense of our vulnerability.

MODERATOR: In organizations that are not using phishing email tests regularly, we've seen the click rate as high as 30% or more. The average test phishing email click rate I'm seeing across the country is about 15% for health care; getting it below 10% is good and below 5% is excellent. But remember, as I relate to CEOs, even if you're below 5%, that still means one in 20 are clicking on phishing emails, which could be part of a larger campaign involving dozens if not hundreds of emails being targeted against your organization.

KELLY WALENDA *(Thomas Jefferson University and Jefferson Health):* I just wanted to add to what we're doing. Mark and I work together. He does a lot of our engineering contracts. I oversee our privacy program. Our CISO and the security team check the supply chain, including all our vendors who are out of the country, regardless of the country.

All the service-line leaders were told to reach out to those vendors they work with, and ask them about their security. When was the last time they had a check? Ask them about patches. They've done that historically, depending on the threat, but they are doing that.

Our security team is also getting reports from the government, the FBI, etc. They start their days around 4:30 a.m. to look for any trends so that they can look for any possible vulnerabilities in our environment.

MODERATOR: Thanks Kelly, and to your point a great deal of cyberrisk is related to third- and fourth-party cyberrisk. For example, third parties, should be queried regarding who their subcontractors are and if they are located overseas — Russia, Ukraine, China, India? Business associates, including their subcontractors, which are based in high-risk nations increase cyberrisk to the covered entity significantly.

SPONSOR

BlueVoyant

BlueVoyant delivers purpose-built cybersecurity services that proactively defend hospitals of all sizes against today's threats by utilizing large, real-time datasets with industry-leading analytics and technologies. We realize that patient data is some of the most confidential and valuable data out there.

Our threat intelligence data detects your most potent cybersecurity risks. At the same time, intuitive automation mitigates threats against your attack surface effectively and efficiently, providing the business and technical outcomes you need to stay secure and support your business objectives.

Our highly-skilled team brings a unique and diverse range of backgrounds and front-line experience to the table, including former government cyber officials from organizations such as the National Security Agency, Federal Bureau of Investigation, Unit 8200, GCHQ, and seasoned veterans from across the cybersecurity industry.

FOR MORE INFORMATION, VISIT:
BlueVoyant.com

American Hospital Association™
Preferred Cybersecurity Service

BlueVoyant is an **American Hospital Association Preferred Cybersecurity Service Provider** for cyber risk management services and managed detection and response services.