American Hospital Association™

Advancing Health in America

KNOWLEDGE EXCHANGE

Monitoring and Mitigating Third-party Cyber Risks

Proactive strategies for managing vendor cybersecurity gaps

Sponsored by: Cybersecurity

Monitoring and Mitigating Third-party Cyber Risks

Proactive strategies for managing vendor cybersecurity gaps

In today's hyperconnected health care environment, a health system's cybersecurity is only as strong as its weakest link, which increasingly includes third-party service providers, mission-critical technology and the digital supply chain. Recent cyberattacks targeting hospitals and health care providers have exposed a critical vulnerability: third-party vendors with poor security practices. When a single vendor's systems are compromised, attackers can gain access to sensitive patient data, disrupt operations and even put lives at risk. This Knowledge Exchange e-book explores how leading hospitals and health systems are strengthening vendor risk management to assess, monitor and mitigate third-party cybersecurity risks before they become full-blown crises and to safeguard patient trust, operational continuity and financial stability.

Action Items

9 ways health care organizations are adopting a more proactive and strategic approach to cybersecurity

1 | **Start with strong governance.** Establish clear oversight, accountability and executive sponsorship for third-party risk. Elevate cybersecurity to ensure that it has the visibility and influence needed — ideally reporting outside of information technology (IT).

2 | **Build a comprehensive inventory.** Identify and document all third-party vendors. Track what percentage of vendors are inventoried and reviewed regularly. Use key performance indicators (KPIs) to monitor progress and accountability.

3 | **Assess risk beyond the third party.** Consider fourth- and fifth-party relationships, as each layer introduces additional complexity and risk.

4 | **Integrate risk into contracts early.** Use proactive, robust contract language to set expectations and enforce standards from the start. Ensure that vendors can demonstrate compliance and not just claim it.

5 | **Prioritize business and clinical continuity.** Understand the operational impact if a third-party system fails. Treat cyber disruptions like natural disasters; plan for both physical and technological emergencies.

6 | **Foster cross-functional collaboration.** Strengthen coordination among procurement, legal, compliance, IT and cybersecurity. Empower teams with clear roles, escalation paths and access to critical contacts (e.g., FBI, internal security leads).

7 | **Use external validation, not just self-assessments.** Don't rely solely on vendor self-certifications. Use independent third-party assessments and corroboration. Regulators expect your organization to perform its own due diligence.

8 | **Leverage industry tools and certifications wisely.** Certifications like HITRUST [Health Information Trust Alliance Common Security Framework] can help, but they're only snapshots. Use platforms that offer real-time risk posture to accelerate procurement and improve accuracy.

9 | **Measure what matters.** Track metrics like inventory completeness, review frequency and executive engagement. Use these KPIs to drive continuous improvement and accountability.

Participants

Paulette Davidson, MBA, FACHE, CMPE
President and CEO
Monument Health
Rapid City, S.D.

Jonathan Ehret, CISSP, CISA, CTPRP, CRISC
Vice President, Ecosystem Risk Solutions, Mastercard
Murray, Utah

Brian Gragnolati
President and CEO
Atlantic Health System
Morristown, N.J.

Ajay K. Gupta, CISSP, MBA
Chair
Trinity Health Mid-Atlantic and Holy Cross Health
Silver Spring, Md.

Wendy Horton, PharmD, MBA, FACHE
CEO
UVA Health University Medical Center
Charlottesville, Va.

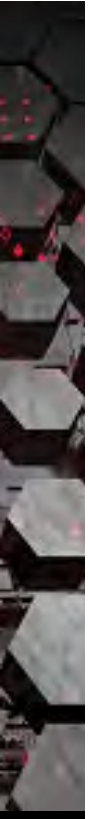
James Leonard, M.D.
President and CEO
Carle Health
Urbana, Ill.

Carlos Migoya
CEO
Jackson Health System
Miami

Candice Saunders, FACHE
President and CEO
Wellstar Health System
Marietta, Ga.

Michael Ugwueke, MPH, DHA, FACHE
President and CEO
Methodist Le Bonheur Healthcare
Memphis, Tenn.

MODERATOR
John Riggi
National Advisor for Cybersecurity and Risk
American Hospital Association
Washington, D.C.



MODERATOR JOHN RIGGI *(American Hospital Association):* **Looking ahead, how is the third-party, mission-critical technology and digital supply chain risk landscape for health care organizations evolving? What emerging threats should hospital leaders be preparing for now? What vendor cybersecurity gaps still exist?**

BRIAN GRAGNOLATI *(Atlantic Health System):* Cybersecurity no longer can be an afterthought in health care; it must be built into our technology by design. Historically, we haven't scrutinized third-party vulnerabilities enough during purchasing, but recent events have been a wake-up call. At Atlantic Health System, we've made cyber risk our No. 1 priority in enterprise risk management. It's not just about certifications or labels; it's about asking the tough questions, digging deeper and ensuring that vendors are truly committed to security. The financial and patient data impacts are too great to ignore. We can't afford short memories — we must stay vigilant.

WENDY HORTON *(UVA Health University Medical Center):* The recent wake-up call has made it clear that health systems must take a more proactive approach to cybersecurity. Many of us have allowed third-party vendors to bolt onto our electronic health records (EHRs) — whether it's Epic, Cerner or another system — introducing additional risks that need to be managed. Moving forward, we need to prioritize the integrity of our core EHR platforms first, minimizing external dependencies that could create vulnerabilities.

Additionally, every major transition, whether acquiring a new hospital or implementing new technology, should be treated as an opportunity to reassess security from the ground up. At every stage, we must resist the temptation to cut corners and instead ensure that everything entering our systems is thoroughly vetted and secure.

MODERATOR: What I'm hearing is the importance of addressing risk at a strategic level — anticipating strategic risks, which then inform technical and tactical risks. A key part of that is understanding who has access to your data. We often assume all our data are contained within the EHR, but in reality, it's everywhere.

CANDICE SAUNDERS *(Wellstar Health System):* I'd add two key points to Brian's insight. First, it's not just about new technology acquisitions — it's equally important to reassess existing agreements. Some of these partnerships have been in place for years, and we've seen vulnerabilities emerge because we assumed our partners were keeping up. But the reality is, you can't just expect it; you have to trust but verify. When we went back and reviewed long-standing agreements, we uncovered risks we hadn't anticipated.

Second, artificial intelligence (AI) introduced another layer of complexity. Even when we thought we were managing it, we realized that outside partners were already using AI without clear rules of engagement. This was especially true with the EHR, where we had to go back and define expectations around AI usage within the platform.

Ultimately, it's about conducting a full sweep — evaluating both current and new systems. In mergers and acquisitions, technology integration is always a top priority, but we had to slow down and be extra cautious. We couldn't afford to inherit cybersecurity risks from a new partner, especially when its outdated

CANDICE SAUNDERS | WELLSTAR HEALTH SYSTEM

// Ultimately, it's about conducting a full sweep — evaluating both current and new systems. In mergers and acquisitions, technology integration is always a top priority, but we had to slow down and be extra cautious. We couldn't afford to inherit cybersecurity risks from a new partner, especially when its outdated systems were part of the reason for the acquisition. //

systems were part of the reason for the acquisition. To maintain our high cybersecurity standards, we accelerated investments in our EHRs and business operations, ensuring that everything was brought in at once. It created pressure on operators and investment priorities, but it was necessary. A weak link can compromise the entire system, so we've learned to go back to basics and never assume anything.

HORTON: And how often are you conducting that sweep?

SAUNDERS: We now conduct annual reviews due to the rapid pace of technological change. Our cybersecurity leaders stressed that with AI, we can't wait for a problem to arise before defining roles and responsibilities. We need clear oversight from the start.

MODERATOR: Especially with AI, it's not always a new vendor introducing it. Sometimes it's simply added as a feature in existing technology, and suddenly it's embedded into your systems.

PAULETTE DAVIDSON *(Monument Health):* We've moved to a single platform for efficiency and cost-effectiveness. Now we're looking at third-party vulnerabilities. We're assessing cyber risk monitoring, reviewing third parties annually and tracking where data is stored— even midyear changes. We're standardizing contracts to require notification of changes and the right to audit, but this puts a heavy burden on us.

JAMES LEONARD *(Carle Health):* What's been shared reflects our experience as well. As large systems, we're fortunate to have the resources to develop these programs, but independent hospitals and many others don't. Too often, decisions are based on availability, cost and vendor support rather than safety and security. That's why it's essential for the entire health care sector to align — because we're all connected, and a single vulnerability can impact everyone.

AJAY GUPTA *(Trinity Health Mid-Atlantic and Holy Cross Health):* That's a great point about the difference in size and scale between systems and independent providers, but maybe it shouldn't be that way. Our core mission is to care for the sick and heal. Should we really be diverting resources to areas that don't directly support that mission? At some point, the broader industry needs to take on the responsibilities that fall outside our core purpose. We're not asking others to heal patients; we do that. But we need the rest of the ecosystem to step up so we can stay focused on saving lives.

MICHAEL UGWUEKE *(Methodist Le Bonheur Healthcare):* While we're getting better, the bad actors are, too — and vendors remain a major vulnerability. It starts with contracts. We need strong language that ensures transparency around changes, acquisitions and especially data storage. My biggest concern is where our data are hosted. For example, when one of our vendors was up for renewal, we learned that some data were stored offshore — something we prohibit without board approval.

GRAGNOLATI: The work John has led — alongside our collaboration with the FBI, Cybersecurity and Infrastructure Security Agency (CISA) and others — has laid the foundation for a more unified approach and helped educate the field in meaningful ways. But we can't assume others will simply 'step up.' Time is

BRIAN GRAGNOLATI | ATLANTIC HEALTH SYSTEM

// We're seeing a growing need to share information, collaborate on common challenges and rapidly disseminate critical messages. One of the most important shifts we've made as an organization is immediately engaging with John, CISA and the FBI when an issue arises. That used to feel like a last resort. Now, it's essential. Ultimately, this work impacts patient care, and there's nothing more important than protecting that. //

critical, and the real challenge now is how we mobilize ourselves to confront the known unknowns. How do we adjust to a potentially shifting governmental approach while maintaining the strong connections we've established, particularly with CISA?

The Joint Commission is beginning to think about this differently. The question becomes: Can we find ways to align efforts across organizations? When you consider the Joint Commission's influence, especially around conditions of participation, there's significant potential to create more cohesive strategies.

From multiple angles, we're seeing a growing need to share information, collaborate on common challenges and rapidly disseminate critical messages. One of the most important shifts we've made as an organization is immediately engaging with John, CISA and the FBI when an issue arises. That used to feel like a last resort. Now, it's essential. Ultimately, this work impacts patient care, and there's nothing more important than protecting that.

LEONARD: Brian, you may recall from our AHA Strategy and Innovation Committee discussions a couple of years ago, that we talked about establishing sort of a 'Good Housekeeping Seal of Approval,' a framework for setting clear criteria. That conversation spoke to the idea of meaningful oversight — taking ownership, not necessarily of the entire technology landscape, but of the parts we can influence. It may be time to revisit it.

DAVIDSON: If the systems we've long relied on are changing or no longer being updated, that's concerning. In response, we developed our own internal risk matrix based on four indices: the Cyber Exposure Index, the Global Cybersecurity Index, the National Cyber Security Index and the Department of State's Travel Advisory. We translate these into a color-coded Excel tool with a defined scoring methodology that evaluates all software vendors across several key attributes. If a tool scores too high — into the red zone — we have to make hard calls and sometimes walk back prior commitments. Our information security team conducts regular audits based on assessed risk levels. The higher the risk, the more frequently we audit.

JONATHAN EHRET *(Mastercard):* What you've built is essentially an inherent risk framework, and not many organizations, even outside health care, are thinking about scoring vendors the way you are. One suggestion: Consider extending that approach beyond just tech vendors. There are nontechnical partners you may critically rely on, and applying the same lens to them could be valuable.

MODERATOR: This is where we distinguish between what's mission-critical and what's life-critical.

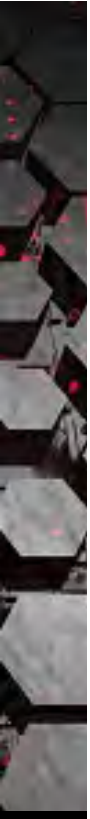
CARLOS MIGOYA *(Jackson Health System):* We've been working closely with procurement and our chief information office to vet not just third-party vendors, but also the individuals within them who may have direct access to our systems.

Our research partners at the University of Miami don't have direct access to our EHRs. Instead, we've created a secure intermediary layer that shares only the clinical data needed for research, excluding any identifiable patient information.

One of the key challenges we face, and one I've seen in other groups to which I belong, is learning from each other's experiences, especially when incidents occur. We need better visibility into where vulnerabilities have emerged across the board and how we can

JAMES LEONARD | CARLE HEALTH

// Our current preparedness exercises and tabletop sessions don't go nearly far enough. They rarely get into the gritty realities where phones are down, systems are offline and you're operating with paper and pencil. That's the real world. //



collectively respond. We need a trusted network to share that information. Our third-party vendor helps assess what we're doing as well as what others are doing. That said, it's still not enough.

MODERATOR: **I see multiple layers to effective information sharing. At the strategic level, we need to ask: Where is the risk really coming from? We've made progress on the technical side of threat sharing, especially through our work with Health-ISAC (Information Sharing and Analysis Center). But at the executive level, we're still lagging. There's a federal law that allows for regulatory and civil immunity when sharing cyber threat intelligence. It's up for renewal in September and we're advocating another 10-year extension.**

What we really need is a faster, more consistent way for leadership teams to share evolving threat information with one another. That's where the gap is and that's where we need to focus.

SAUNDERS: We've seen vulnerabilities with some of our university partners, particularly as we train their students and grant access. Contract labor introduces additional exposure.

With Change Healthcare, speed was critical. At first, the vendor offered no acknowledgment, leaving us in the dark. When accounts receivable are at risk, there's simply no time to wait. Larger systems like ours could mobilize quickly. That's the tension we constantly manage, making sure that patients get care while navigating fragmented communication and an increasingly unpredictable threat landscape.

MODERATOR: **To reinforce your point, we're advising hospitals to treat cyber incidents like any other regional disaster, like a hurricane, flood, fire or mass casualty event, because their impact often extends across regions as patients are diverted. We're also recommending that organizations revisit their existing emergency management plans. There's no need to create a new plan. In fact, most emergency management plans, mutual aid agreements and emergency protocols already account for cyber-related events.**

We're urging those leading cyber incident-response planning to integrate their efforts with emergency management, because these aren't just isolated IT issues, they're regional disasters.

We're making it clear to the federal government that ransomware attacks aren't simply data theft; they're threats to life and must be treated as such.

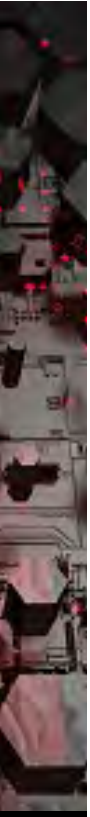
EHRET: At Mastercard, one of the things we do is assess companies' cyber posture from the outside. We've analyzed every breach and ransomware event over the past nine years, scoring them objectively. And even among companies rated 'A' for security, 5% still experienced a breach or ransomware event.

Sometimes it's just a single click on a phishing email. The truth is, even with top-tier defenses, incidents still happen. But there's a shame-based culture that creeps in — the idea that if you've been breached, something must be fundamentally wrong.

DAVIDSON: The bad actors are already using AI to scan for vulnerabilities across our health systems, companies and critical infrastructure. Is there AI to fight AI?

PAULETTE DAVIDSON | MONUMENT HEALTH

// We began this journey last year when our board designated business continuity as our transformation project. The goal was clear: Identify critical functions across our hospitals and clinics, build a comprehensive continuity blueprint and test it. Going through the process was eye-opening. The experience was incredibly educational, not just for me, but also for our board and leadership team. //



MODERATOR: There is offensive and defensive AI. You might already have it.

LEONARD: Our current preparedness exercises and tabletop sessions don't go nearly far enough. They rarely get into the gritty realities where phones are down, systems are offline and you're operating with paper and pencil. That's the real world.

I also want to revisit that phrase — 'a 9/11 mentality.' The day after 9/11, we were already thinking about anthrax, smallpox and how to regionalize care, how to keep emergency departments open even if it meant posting armed guards. It was a mindset rooted in survival and coordination, a cooperative approach to ensure that we can still treat heart attacks, strokes and anything else if the worst happens and only a few systems are left standing.

MODERATOR: We're applying incident-command principles and running regional exercises now in states like Texas, Louisiana and Florida — places already experienced with hurricanes and natural disasters. They have strong regional response plans in place. The difference now is, we're saying: 'This isn't a hurricane, it's a digital storm.' One or two hospitals could be knocked offline. And they understand that. They start planning for patient diversion and service continuity. We're not reinventing the wheel. We're just adapting proven disaster frameworks to meet the cyber threats of today.

DAVIDSON: We began this journey last year when our board designated business continuity as our transformation project. The goal was clear: Identify critical functions across our hospitals and clinics, build a comprehensive continuity blueprint and test it. Going through the process was eye-opening. The experience was incredibly educational, not just for me, but also for our board and leadership team.

It's been resource-intensive — pulling staff from operations, hiring a blueprint manager and constantly updating plans that quickly become outdated. But we've seen firsthand why it matters. About a year ago, our EHR began lagging. We made the call to shut down the network. It turned out to be a server issue, but we were down for eight hours. That unplanned outage was a wake-up call.

Since then, we've implemented dual server locations and expanded our preparedness efforts. We're even training caregivers to operate on paper when systems go down.

MODERATOR: No matter how much we invest in defense, we could spend our entire budget on cyber and still not be immune. That's why we're urging health systems to shift their focus beyond business continuity and start planning for clinical continuity. If technology goes down, how will we continue to deliver safe, quality care for 30 days or more? You won't have everything, because the tech stack is vast, but you must identify your core technologies: the life-saving, life-sustaining systems, and the mission-critical functions like payroll and revenue cycle. That's where your recovery strategy has to begin.

SAUNDERS: Patching has become an operational burden and a real vulnerability. These patches aren't just internal; they stem from our vast web of external relationships, and keeping all those systems updated

MICHAEL UGWUEKE | METHODIST LE BONHEUR HEALTHCARE

// Pay close attention to the contracting process, ensuring that risk considerations are embedded from the start. For the most critical areas, assign an accountable executive in addition to the cybersecurity roles to maintain visibility and oversight. Just like executive sponsors are assigned to key initiatives, these leaders help to ensure sustained focus on high-risk, third-party relationships. //

is a constant lift. We've started asking the tough questions: Do we really need 10 different versions of the same kind of technology? We've tried to limit what's introduced into the environment in the first place. But even with that, the risk is real.

I used to wonder, 'Can't we just stop all the patches?' But you quickly learn that it's not that simple. Sometimes you need a patch for the patch. And external agencies are starting to scrutinize how we manage these updates, what our process is and how we mitigate the risk they carry.

HORTON: If an organization has limited resources and must choose between investing in continuity planning or strengthening upstream governance — like contract oversight and preparedness — what should take priority? It's a tough decision; both are critical.

MODERATOR: Based on what we've covered, what would you say are the top three priorities for third-party risk management? Effective third-party risk management starts with strong governance — establishing clear oversight and accountability. It also requires a deep understanding of the technology being adopted: what it does, the risks it introduces, and the potential impact if it fails. This insight directly informs business and clinical continuity planning. By recognizing the consequences of losing access to mission-critical, third-party systems, organizations can better prepare and strengthen their continuity strategies.

UGWUEKE: Start by creating a comprehensive inventory of all third-party vendors with whom your organization engages. Once that's established, assess and categorize them based on each of their levels of risk. Pay close attention to the contracting process, ensuring that risk considerations are embedded from the start. For the most critical areas, assign an accountable executive in addition to the cybersecurity roles to maintain visibility and oversight. Just like executive sponsors are assigned to key initiatives, these leaders help to ensure sustained focus on high-risk, third-party relationships.

GRAGNOLATI: It's not just about third-party vendors anymore. We need to think beyond that. We're also dealing with fourth-party and even fifth-party relationships. Each layer adds complexity and potential risk that must be accounted for.

MODERATOR: Brian, to your point, take the Change Healthcare incident. Some organizations said, 'We don't even use Change, so why are we down?' Their clearinghouse did. That's the hidden risk of downstream dependencies.

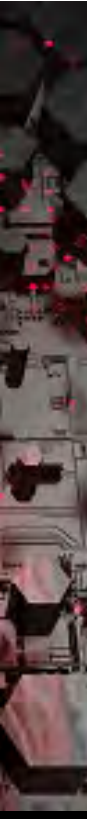
SAUNDERS: We realized we had to be intentional about both physical and cyber/technology risks. That led us to bring our physical security and cybersecurity teams together to collaborate more closely, recognizing the growing risks in health care. Ultimately, physical and cyber risks are deeply interconnected, and both need to be treated as strategic priorities.

Another key move was shifting cybersecurity out from under IT. While IT had good intentions, cybersecurity's voice often wasn't loud enough when it came to prioritizing investments. By elevating it to report directly to me, we gave it the visibility and influence it needed.

DAVIDSON: You're right. We need strong, proactive contract language with every vendor—third party

JONATHAN EHRET | MASTERCARD

// Self-certification can be misleading. There are platforms and exchanges that offer pre-completed assessments, which can help, but the responsibility still falls on you. Regulators won't accept 'Another organization reviewed them, so we didn't have to.//



or beyond—to ensure that they meet our standards and can prove it. Vendors often go straight to our physicians and caregivers with the latest innovations, which puts us on the defensive.

If we educate our teams on what to look for in a vendor and align that with our contract terms, we can avoid reinventing the wheel. With the EHR, enterprise resource-planning system and more than 150 other applications, it's a constant, dynamic evaluation process.

EHRET: The real risk is with tools we don't even know are being used —like someone independently launching a survey on SurveyMonkey that collects protected health information. In those cases, the contract is between the physician and the platform, not us. We don't have access to the data and we have no rights to it.

MODERATOR: Where does third-party risk management sit within your organization? How does it intersect with functions like cybersecurity, legal and compliance? And how is that collaboration structured and managed in practice?

DAVIDSON: In our organization, information security falls under corporate responsibility alongside compliance and internal audit. It works closely with legal, which leads broader risk management. Corporate responsibility reports directly to the board — not to me — but the senior leader often brings issues to my attention so we can align. They're accountable to the board's corporate responsibility committee.

HORTON: This level of collaboration among procurement, legal, compliance and IT is new for us just in the past year. It feels different, more integrated. Have we truly empowered our teams to make critical decisions? Do they have the right contacts — like your numbers, or even the FBI's — readily available if something happens? I'm not sure every hospital is prepared that way."

LEONARD: Operations is where the impact will be felt first. When a crisis hits, the ops teams move fast. We have to be careful that our cybersecurity protocols don't unintentionally slow them down or overlook urgent patient care needs. It's critical to build a bridge between cybersecurity and operations, whether through representation, the CEO's office, or another channel, so both priorities are aligned and supported in real time.

SAUNDERS: We've found that treating a cyber event like a natural disaster or major incident helps set the right pace. It immediately shifts the focus to assessing the threat. That's what operators need to know: Is this serious enough to stop surgeries? Do we keep systems running?

You have to move quickly to define the threat and determine the response. If not, frustration builds fast across teams that are trying to make critical decisions without clear guidance.

MODERATOR: We've touched on measuring third-party risk, and there are tools and external resources available. But if you had to prioritize, what key metrics would you focus on? Surveys provide a helpful snapshot, but how would you measure third-party risk dynamically over time? As a leader, what are the top two or three indicators you'd rely on to assess and manage that risk effectively?

UGWUEKE: I'd start by creating a KPI focused on inventory: What percentage of our third-party assets

PAULETTE DAVIDSON | MONUMENT HEALTH

// If we educate our teams on what to look for in a vendor and align that with our contract terms, we can avoid reinventing the wheel. With the EHR, enterprise resource-planning system and more than 150 other applications, it's a constant, dynamic evaluation process.//

have been identified and documented? Are we at 90%? 70%? That gives us a baseline. From there, we can set goals around review frequency and ownership. Another KPI could track how often these reviews are brought to senior leadership or cybersecurity for action. It's about setting clear targets, monitoring progress and ensuring accountability

DAVIDSON: Is there an industry standard for those vendors conducting their own risk assessments?

EHRET: I'd caution against relying solely on vendor self-assessments; self-certification can be misleading. There are platforms and exchanges that offer pre-completed assessments, which can help, but the responsibility still falls on you. Regulators won't accept 'Another organization reviewed them, so we didn't have to.' I've seen that firsthand in finance; each entity still had to do its own due diligence.

That said, using pre-assessments and technologies that provide real-time risk posture can speed up procurement significantly, especially for long-tail vendors that typically take months to onboard. It's far more effective than relying on a questionnaire filled out by a sales rep who just checks every box 'yes.' Accuracy matters.

There's the HITRUST certification, which some health care organizations require from vendors. It's often treated like a 'Good Housekeeping Seal of Approval.'

MODERATOR: **Just as in any investigation, you need independent third-party corroboration. Whether it's on your side or the other's, it has to be objective. You might identify a portion of the risk, but without external validation, you can't fully understand or mitigate it.** ●

Sponsor

Cybersecurity

Mastercard Cybersecurity

At Mastercard, we understand that managing cyber risk isn't about a single goal — it's about enabling organizations to assess, protect and organize with confidence.

Our cybersecurity solutions extend far beyond payments, helping organizations secure their infrastructure, applications, third parties and global supply chains. By providing deep visibility into risk across internal systems and external relationships, we empower businesses to identify vulnerabilities before they become threats. Through unique threat intelligence and multi-layered, cloud-based defense technologies, Mastercard helps organizations and consumers address risk in real time, enhancing resilience against today's most sophisticated cyberattacks.

LEARN MORE ABOUT MASTERCARD CYBERSECURITY SOLUTIONS:

www.riskrecon.com