Podcast Transcript

Regulatory Horizons: Cybersecurity and FDA Regulated Companies

Date: February 10, 2026

Guest: Winston Kirton and Eric Gyasi, **Host:** Amy Kattman

Run Time: 24:14

For questions and comments contact:

Winston S. Kirton

Partner
Washington, D.C.
T: +1.212.861.1715| wkirton@bakerlaw.com

Eric B. Gyasi

Partner
New York
T: +1.212.271.1514 | egyasi@bakerlaw.com

Kattman: Welcome to Regulatory Horizons, delivering strategic insights for the future of global life sciences regulation. This podcast is your guide to the evolving policies, global frameworks, and innovations shaping the compliance landscape across biotech, pharma, medical devices, and even foods. I'm Amy Kattman, and you're listening to BakerHosts.

Cyber threats are growing, FDA expectations are rising, and companies are scrambling to stay ahead. Today on Regulatory Horizons, we're unpacking what all of this means for patients' safety and regulated products. Let's listen in.

Kirton: Hello, friends. My name is Winston Kirton, and I am the leader of BakerHostetler's FDA practice and co-leader of the firm's Life Sciences Industry team, and the host of the Regulatory Horizons podcast.

Cybersecurity is no longer just an IT or privacy issue. For FDA-regulated companies, it is a patient safety issue, a product quality issue, and increasingly, a regulatory enforcement issue. FDA has made it clear that cybersecurity vulnerabilities can affect medical devices, software, manufacturing operations, clinical data, and even the availability of life-saving products. Today, we're bringing together two perspectives, the FDA regulatory lens and the cybersecurity lens. We're bringing them together to talk about what companies need to understand and where they're getting tripped up.

I'm delighted to be joined by my partner, Eric Gyasi. Eric strategically guides clients to address cybersecurity enterprise risks and proactively implement cybersecurity governance frameworks. He advises clients on compliance with complex state, federal, and sector-specific cybersecurity regulatory requirements in a risk-informed manner. A strategic thinker valued for his business-minded judgment, Eric advises boards of directors regarding the duty of oversight related to cybersecurity governance. With both his crisis communications experience and his digital forensics background, Eric is uniquely qualified to help clients navigate the legal and business risks at the intersection of incidents response and regulatory enforcement. Welcome to the Regulatory Horizons podcast, Eric.

Gyasi: Thank you, Winston. I appreciate it. I'm happy to be here today to share my thoughts on the intersection of cybersecurity, governance, and FDA-regulated companies.

Kirton: Wonderful. So, let's jump right in, right? So why is cybersecurity an FDA issue? As you know, FDA doesn't regulate, quote, unquote, cybersecurity as a standalone concept, right? It regulates safety, effectiveness, and quality. So, from your perspective, why do regulators care so much about cyber risk at this point in time?

Gyasi: So, Winston, your framing is exactly right, and it mirrors how the FDA frankly thinks about this issue, because cybersecurity matters because it affects the product trust across an entire life cycle. So, where I sit, we see cyber risk, and you see devices are disabled, or you compromise software functionality, or manipulate data, and or interrupt manufacturing operations that the FDA views as integral to the safety and quality. So really what we've seen is over the last several years, the FDA has made it clear that cybersecurity isn't a bolt-on. It is to be embedded in design controls, quality systems, and post-market oversight.

Kirton: Yeah, it seems like there is some sort of a trust issue in all of this. And my interpretation is that from FDA standpoint, a loss of trust can translate directly into adulteration or a quality failure and even with patient harm, right? So, is this aligning with what you see in practice?

Gyasi: It aligns completely. In practice, I'd say the FDA is less focused on whether a cyber incident caused immediate harm and more focused on whether a company can demonstrate control and risk management. So, we routinely see cyber issues that are reframed through inspections as a quality systems breakdown. So, three ways, risk assessment gaps, validation failures, or frankly, weak

change management. So that is why the FDA can treat these adulterations or non-conformance issues even without patient impact. If you get a little bit more specific, I'd say in pharma, FDA often looks at whether system compromise undermines confidence in batch records, testing data, or release decisions, all of which step beyond an immediate incident response.

Kirton: Yeah, that is right. And where companies are getting it wrong is that, my impression from what I'm seeing, companies are not realizing that they have a cybersecurity problem until FDA starts asking questions, right? So where do you typically see, in that list you gave out, where do you typically see the biggest gaps?

Gyasi: Your question made me chuckle, Winston, but I would say the most common gap is that cybersecurity in many ways, it is still siloed in IT rather than embedded in the product and the quality life cycles. And so, what is the takeaway there? Companies may have controls, but they haven't mapped those cyber risks to specific products, manufacturing processes, or regulated data streams that the FDA may evaluate. A close second is over-reliance on third parties. Now look, the FDA's posture is clear. The regulated entity owns the risk, even when vendors are deeply involved. And so more specifically, we oftentimes see device manufacturers that focus on network security, but they under invest in secure software design or post-market monitoring.

Kirton: So, one thing FDA often focuses on is whether a company can demonstrate control, right? Not whether it has a perfect security approach or strategy, right? It is really around control, control of the manufacturing process, control of the clinical process, control, right? That is a big word with FDA. So how often does documentation become a problem in demonstrating control?

Gyasi: Well, Winston, I'll start with your use of the phrase, perfect security. Reminds me of a quote, don't compare me to the almighty, compare me to the alternative. I would say here, the FDA isn't expecting perfect security. But what is the FDA expecting? It is expecting evidence of governance and decision-making.

To stress the point, it isn't that something won't go wrong, but the FDA's key to figure out did we have the correct governance in place? Did we have the correct decision-making in place? So, it is not necessarily the outcome or the output, but rather what was the inputs that went into the particular incident we had? So, when cybersecurity isn't integrated into quality systems, documentation gaps emerge quickly to the point you're asking. So, companies may be acting reasonably, but if they can't show how risks are assessed, they can't show how security incidents are escalated, and they can't show how security incidents are addressed, the FDA loses confidence in the control environment. And when you think about it more specifically, for pharma companies, missing documentation around validated systems and corrective action, candidly, is what often drives regulatory scrutiny.

Kirton: Yeah, it is interesting, right? Big companies have resources and you would think they have it figured out. As you know, Eric, I have several startup clients, right?

And they sometimes argue that they don't have the resources and the insights. But how do startups misunderstand the cybersecurity expectations of regulators like FDA, for example?

Gyasi: Well, Winston, as a dad of two kids, I've always been told you can't punish one and let the other one get off scot-free. So, let's not assume that the large companies have it all figured out and it is just merely a startup client's issue. But we'll focus it right on the startup piece where you started.

Look, startups often assume cybersecurity comes with approval, right? But the FDA guidance makes clear that cyber risk is expected to be addressed early. So, it is much easier to course correct before the train leaves or immediately after the train leaves the station, rather than when the train is much, much further down the track. So, to bring it back here, how does it play? Especially in software development, system architecture, or design controls. Those should be addressed at time zero and not, as I said earlier, further down the track.

The FDA doesn't expect startup scale companies to look like global enterprises. but it does expect risk-based thinking and documentation from day one. So, we're thinking about, for instance, devices. This comes up most often with software-driven devices where security decisions made early are hard to unwind later. Because at the end of the day, when you create or pull together software for a device, it doesn't really matter if you're a startup or global enterprise, security should be centered in that development lifecycle.

Kirton: Yeah, that is right. That is right. Let's pivot a little bit to cyber incidents and FDA risks, right? The moment of truth, as you and I have discussed from time to time, is often after a cyber incident, right? After the issue has hit and everybody is scrambling, and they often really hit at inopportune times, right? So, from your perspective, when does an incident become an FDA issue?

Gyasi: Well, to your point about inopportune times, I'm still waiting for the security incident that takes place Monday morning at nine a.m., but unfortunately not. They're usually Saturday afternoons, Thursday nights. So, but I digress. Look, an incident becomes an FDA issue when it affects, or really could reasonably affect, product performance, data integrity, or manufacturing continuity. Even incidents that start in corporate IT can quickly implicate regulated systems. And that is something you and I have dealt with when it starts on one side and pivots to the other.

Kirton: Right.

Gyasi: The FDA looks past the initial event and where they focus, whether the incident reveals deeper governance or control weaknesses across their life cycle. And I realize I may become a bit of a broken record, but really it is that governance and control weaknesses that the FDA starts to lens in on. So, if you think about a large pharma or biotech company, large or small, for many of those companies, manufacturing disruption or data integration concerns are really what brings the FDA into the conversation.

Kirton: Right. It is not lost on me that from FDA's perspective, potential patient risk matters, right? It is not even just the actual, the potential, right? It is the prevention. So even if no harm occurs, there is still a desire to protect, right, that harm from really permeating into something larger. So, do companies tend to underestimate the risk?

Gyasi: So, Winston, this is a callback to the earlier question and answer when I said they're less focused on the outcome because to your point, the fact that you had a near miss or something bad didn't happen is not sufficient from the FDA's perspective. And yet for many companies, near misses are routinely underestimated. So internally, teams move on once systems are restored, whereas the FDA, frankly, views near misses as an early warning sign of systemic risk. What matters is not just what happened, but what could have happened under slightly different circumstances. Then when you think about what is at play, potential patients, it really behooves the FDA to focus on what could have happened, and it behooves the companies in question here to focus on that as well, too. Having a near miss in this case isn't a cause for celebration or frankly, as I said earlier, turning the page, but rather it is an alarm for companies to reassess and to dig deeper as to what potential systemic risk may exist.

Kirton: Yeah, it is a challenge, right, for some companies to get into that mindset. From your experience, Eric, what incidence response mistakes tend to increase regulatory exposure?

Gyasi: So that is a great question. And I have a short answer and a long answer.

Kirton: Give me both.

Gyasi: Two for the price of one. So, the short answer, if you will, is that incident response these days are cross-enterprise issues. And where it becomes a big mistake is when companies or information security teams think of incident response as a purely technical exercise. What I mean by cross-enterprise is that quality, regulatory, and legal teams ought to be engaged early and decisions have to be made with those lenses in place. Because when the FDA is reviewing the steps and actions you as an organization took, they're not going to step back and say, well, this is a great response when you think about it in merely an information security context. No, the FDA is going to look at this from a whole of enterprise response. And so, why would a company hamstring itself during the incident and later on with the regulatory inquiry by not bringing in quality regulatory and legal teams into the fray? And frankly, when you think about it, not doing that creates inconsistent narratives around data integrity. And again, that is what the FDA focuses on after an incident.

Kirton: Thank you. On this podcast, listen, we like to tell people what the story is, but we also like to share what they should be doing or considering, right? So, let's transition to some practicality, right? Let's make this a little bit more practical.

Gyasi: Sure.

Kirton: What are the top two, three cybersecurity priorities for FDA regulator companies that you see right now and understanding that you just don't focus on FDA regulated companies, any other from other businesses or companies you're dealing with that may be regulated?

Gyasi: So, the key message here is that cybersecurity has become a core FDA compliance capability. And again, it is not about perfect security, but it is about the governance, the control, the documentation across the product lifecycle. Companies that embed cyber risk into their quality systems, and importantly, treat it as a continuous loop, are the ones who are best positioned to have a back and forth with regulators.

I'll also add, and I used the phrase earlier, cross-enterprise, this also goes up to both the board and the senior management level as well, too. When I mentioned governance, it is essential. FDA enforcement actions increasingly reflect governance failures, not just the technical ones. And so, when you don't treat cybersecurity as an enterprise risk, that accountability mechanism breaks down. So, it is important that boards need and have that visibility into how cyber risk flows into that cybersecurity loop, from design and validation through operations, response, and continuous improvement. So, to make it a short answer for you, I think it is governance, it is process and documentation, and then proper accountability at the senior management and board levels.

Kirton: Yeah, let's stay here for a little bit on board, right? So, you mentioned governance, you mentioned enterprise risk, you mentioned documentation, you even mentioned training. And of course, all of this should cycle up to the leadership of the organization. Can you give us a sense, from your lens, how important is leadership and board engagement?

Gyasi: I think it is critically important because if you consider what a board is supposed to do or ought to do, a board provides oversight of management and management strategy. Then, of course, beneath management, you have the operational level that implements that strategy. So, without the board's oversight, without the board's, if you will, direction setting, the question is raised, well, what is management strategy really keyed into? And ultimately, how are we then implementing that? So, it is critically important. I would describe it as an arrow that goes both ways. On one hand, the board, by putting its strength and _____ behind it, helps to drive the importance and management focuses on it, and the rest of the team implements it.

But the arrow goes the other way as well, too. It is incumbent upon the operation layer to report accurately up to management and then for management to turn the technical reports into a risk-based discussion that the board understands. No one ever once again is in front of a board and start talking about firewalls, patch management, or vulnerability schedules. That is not what we want. But what ought to happen is management to frame this in a risk-forward posture. Here are the risks, here is how it impacts the business, and here are the costs associated with that. There, the board can then, in its oversight function, decide how much risk are we willing to take? Does this in line with our risk appetite? They can have

the board-level discussions, and then management will translate that into technical implementations for the operational level.

Kirton: Yeah, I think there is some fluidity with management and board engagement, right? However, we also, as I mentioned before, we have a number of clients who are start-ups or emerging companies. And oftentimes we represent investors as well that are investing into those companies. And so, we talked about board and we talked about the management people, but what should investors be asking management around cybersecurity and protections and the like?

Gyasi: Well, first of all, they are ready to turn down the track if they're merely asking these questions. So, let's give credit where credit is due. Investors and boards should be asking these questions, particularly in a startup context, but not all of them are. Now, the ones that are asking the questions, they should be asking whether cybersecurity is tied into product and patient risk. Or as we said earlier, how is it embedded into the quality systems? And finally, how is it tested through incident response exercises that include regulatory decision making across enterprise tabletop exercise, if you will? And so those questions, the reason why I frame those questions, those are the ways in which the FDA will ask those regulatory inquiries, and it aligns with the FDA's expectations, and more importantly, it quickly surfaces maturity gaps. So, when you think about, again, a pharma or a biotech company, boards ought to be asking how cyber incidents would affect manufacturing, release decisions, and regulatory reporting.

Kirton: Yeah, and of course, they do that seamlessly, right? It is a challenge. It is a challenge, right? It is a challenge.

Gyasi: It is a challenge. And to your point about that, we chuckle because we appreciate the challenge and where both a management team, even at the startup level or a board, they need to sync up is what does reporting look like for those groups? Because what an investor is looking to see, what a board is looking to see, what a manager team is looking to see are slightly different. So, where an information security team can work together to determine what does reporting look like for those three stakeholders and ensure that you're reporting in an accurate and in a repeatable fashion and that way, boards can track this quarter over quarter at board meetings, audit committees can dig deeper into this in between their board meetings, and management can ensure that their strategy is aligned with the risk that the company would like to take. So, while we chuckle there, the more serious takeaway is for companies to think through, how do we report to those three key stakeholders?

Kirton: No, that is right. That is right. Alright, it is time to land the plane. I wish we could stay here all day and speak on them because again, I think in some regards it creeps up on companies. In other regards, companies think they have it all figured out. And lastly, some companies, the management and the leadership are not even clear of the fact that they have responsibilities around cybersecurity to the regulator, right?

So, the takeaway here is cybersecurity is no longer a background risk for FDA regulated companies, right? It is a core compliance and business continuity issue. Eric, you mentioned that. FDA is expecting zero vulnerabilities, right? But it is expecting companies to understand, manage, and document risk, right?

Gyasi: Correct.

Kirton: In a way that protects patient and product integrity, right? So, it is twofold, right? We ultimately have to protect patients and those products that are going to be introduced to patients, we have to ensure that they're safe for that purpose. So, the other thing we talked about here, Eric, was for leadership teams, cybersecurity must, right, must, or as lawyers, we tend to say, shall be treated as a regulatory capability, right? It is just not a technical function anymore, right? So, listen, Eric Gyasi, thank you so very much for joining us. And I do look forward to you coming back to share insights soon. I wish we had more time, but thank you.

Gyasi: Winston, you're very welcome. This means I'll have to do a second one of these. Thank you for having me on today.

Kirton: Of course you will. Of course you will. We continue to gather data, my friend, right? We know what is going on in the field, and we're more than happy to help those of our listeners that really need help. And lastly, I want to thank our listeners for tuning in to the Regulatory Horizons podcast. Stay well, everyone.

Kattman: Thank you, Winston and Eric. If you have any questions for Winston or Eric, their contact information is in the show notes. As always, thanks for listening to BakerHosts.