You're listening to the GRC podcast series, the place where industry experts, analysts and veterans help us understand the upcoming cybersecurity technologies and trends. If you haven't subscribed to the channel already do it now for regular updates. In this podcast we have with us Abhishek Ramavat, who will be sharing his views on how enterprises can tackle various challenges associated to third party risk management and the role of technology in mitigating these risks. This episode starts in 321.

I'm sure they would also like to know more on how technology can help improve the speed, scalability and collaboration of vendor risk assessments. Very good question. Let me speak about either speed, scalability and collaboration one by one, right? If you look at the way the digitization is happening, there's an obvious need in the organization that we should be able to onboard third party in a lesser time, right, let's let me let me put that as an example. Now, you know, these assessment processes will become a hindrance, you know, if you really want to look at more agile ways of working more DevOps ways of working, more cloud adoption happening, right. So if we have to put a system where these multiple information sources, multiple workflows, multiple data sources can be integrated, that can contribute significantly into time to be able to assess a third party, right and show a compliance to a third party, right. So that's where technology will play a significant role when it comes to speed in terms of integrating multiple sources in terms of, you know, building a workflow engine to be able to, you know, run it more systematically, in terms of, you know, bringing more collaboration, right in terms of data sources that might exist is something which is very, very important from a speed perspective that technology can bring. The second area, which I think is scalability, and see the number of third parties is increasing, it is becoming 1000s and 1000s. of for every organization, right. And it's not just third party, you know, it also contributes from fourth party first party these days, right. So it is very important that our technology and frameworks that we set up should be able to scale up the volumes that are coming up. If I kind of look at more and more technology vendors who are existing in this space, they have kind of adopted to the scalability problem that might exist in large enterprises, right, or mid sized enterprises. So for example, in terms of I want to release into force, if, you know, for, say, 1530 suppliers or 1520 suppliers, can I do it in a span of a click of a button? Right. So that that should be my scalability options available? Do I have an option of you know, kind of increasing and decreasing my, you know, third party risk? You know, from a scalability perspective? Can I decrease my third party, you know, vendors count, or can I increase them, but that's something which is very important from a scalability perspective. Now, the third is collaboration, if we are able to create decentralized solutions, platforms, and frameworks, where there's a lot of data exchange happening, why do I have to, for example, talk to my third parties, you know, to get their security scores, their sustainability scores and their cyber scores? Can there be a collaborative platform being made, you know, the information is available on a real time basis, you know, it takes feed from multiple sources and vendors are allowed to share their say, for example, this assessment scores, their certification scores their findings in a very, very collaborative way, right. That's where technology will play a you know, humongous role, you know, if the collaboration between organization third parties and fourth parties need to happen, right. Does that make sense?

It absolutely does have a shake, that was very insightful. Can you also share with our listeners some areas and use cases for technology intervention and third party risk management? Sure. So, so, let me first give you a context in terms of what is happening from a technology adoption standpoint, right, as we are talking to customers or partners. So, we see more and more organization looking for a central system to manage third party risk and it is not limited to just se C's organization, it is also getting extended to the chief risk officers You know, there are dedicated roles being created with respect to

head of third party risk, the procurement functions are kind of looking for such solutions more and more. The second key reason for technology adoption is the increased focus from regulator right. So you know, we saw this in the GDPR days we are looking at at in the US when it comes to ccpa or lgpd and

lat am so regulated these days are asking for more control from the organization to look at the third party risk, right. So concepts around continuous monitoring is again one use case, which is, you know, which is needed by organization more and more. The third area, which I want to bring as a context to technology adoption, as is how do we use the publicly available information, right? You know, there are a lot of sources available, where we can probably do some, you know, bring intelligence from web world, we can look at social media as one source of information, we can look at financial performance, you know, there's tons of publicly data available for the enterprises, we can look at sanction lists. So that's where technology can play a significant role from a use case perspective. I think another thing which I want to bring is, you know, correlation of this data, while you know, we know sources we know places where this information is lying. Can we really correlate, you know, can for example, if I am seeing one of my vendor getting constantly beaten upon financial performance, and they are supporting a critical function, when it comes to my organization, can I really correlate that data in terms of doing the assessment on the organization, right, that's, that's something which becomes very critical rates. Similarly, you know, if I look at, say, continuous monitoring solutions, where I can get more context from the web world, in terms of what kind of external facing vulnerabilities are existing, right, for a third party or a supplier, and then relate it back to my third party assessment, that's where technology is playing a critical role. Right. So the typical use cases that we are hearing from our customers is around, you know, with respect to technology adoption is in terms of helping prioritize and cheering of third party vendors, support in the new vendor selection, you know, running ongoing vendor assessments, or third party assessment is looking at, say, critical vulnerability management or weaknesses in the organization's or third parties. How do you monitor response? How do you do continuous monitoring is, again, one of the use cases that we're hearing from our customers? How do we get visibility from the fourth party risks that might exist in which are third parties for the third parties? And what do we bring that data back into, you know, our own DRM processes? Right? So these are a few key areas where we see a lot of organization investing, from a technology perspective, when it comes to third party risk management. lien Does that make sense? It does, it does appreciate? Also, you spoke about how more and more organizations are looking for a central system to manage third party risk management, but what if there are there must be some who are not? And what are the risk of not adopting technology in third party risk management? See, if you ask your mind view, you know, not adopting technologies is not a solution anymore. But if, if certain organizations still want to stay more reactive and more manual, then they're obviously inviting more troubles for themselves. You know, for example, you know, we have seen more and more organizations struggle, if they don't have a very systematic and automated way of looking at third party risks, right? I don't want to quote those instance, you know, incidents, which happened quite recently. So if you look at last six months, a number of breaches, which are, you know, directly relating to lack of technology, which the firms had, right, the second a key area, which I think if if organization do not adopt technology is terms of risk of non compliance that they're carrying, right. And non compliances, to the regulatory requirements, you know, as the regulators are expecting more and more, the exposure is also increasing. So if you really don't bring a technology intervention, then you know, probably, we are inviting trouble for ourselves, right. And then, you know, the business context which is needed in a, in a very effective third party risk management process, you know, that is not possible without an automation, right? For example, linking it back to the organizational impact, linking it back to

my contractual obligations, you know, that cannot be achieved by manual ways of working or ad hoc ways of working, right. You know, if I have to do a financial viability assessment of third parties, and if I don't have these discrete information sources coming together, that's not possible again, then you are kind of keeping living with that risk of not knowing your third party and to end. The other key areas that I see that cannot be achieved without an automation or brings risk around third party is around are you really doing through benchmarking of your third parties within the organization, you know, are really, really looking at your risk? Are you really looking at the publicly available information, right? So that's again, something you know, that you carry as a risk. If you're not automating these processes, or if you're not bringing technology, right technology to be able to run these processes. These are few areas, which I think if are not addressed, you know, but obviously bring more risk to the organizations and having said that, I would still say

You know, we can't move forward Stone Age, technology adoption is not an option. It is a mandate which is needed for the organization's now. It's just a matter of time and the matter of time, you know, exposes you to a number of risks that I just spoke about right.

This episode of The GRC podcast series has ended, but be sure to subscribe for more insights on how to identify, understand and prepare for the world of possibilities around the new and upcoming cybersecurity technologies and trends. Don't forget to rate and review the episode so that we can keep bringing you the most relevant content. Thank you for listening